West African Journal of Industrial & academic research
Vol.10 No.1. April, 2014

West African Journal of Industrial & Academic Research

Computing, Information Technology Research & Production

Mathematics, Statistics, Econometrics and Operations Research

Management, Education & Social Science Research

West African Journal of Industrial & academic research
Vol.10 No.1. April, 2014

West African Journal of Industrial & Academic Research

Publications Office:
9-14 mbonu Ojike Street
Ikenegbu, Owerri, Nigeria
Tel: 234 81219 41139
www.wajiaredu.com

International office:
255 North D Street
San Bernardino, CA 92401
909.884.9000

Published by:

Olliverson Industrial Publishing House
The Research & Publications Division of **Hi-Technology Concepts (WA) Ltd**

For The

International Institute for Science, Technology Research & Development, Owerri, Nigeria & USA

A Review of RSA Cryptosystems and Cryptographic Protocols

[1]Prince Oghenekaro Asagba, [1]Enoch O. Nwachukwu

[1]Department of Computer Science, University of Port Harcour, PMB 5323, Port Harcourt, Rivers State, Nigeria (pasagba@yahoo.com),

ABSTRACT

The use of cryptography in information security over insecure open network in both the convectional / symmetric encryption and the public-key cryptography has witnessed tremendous developments over the years. No doubt, the public-key cryptography is an established technology in terms of modern approach in information security despite the seemingly challenges it has. This paper, gives an overview of the public-key cryptography with emphasis on the RSA algorithm. We examined public-key cryptography, reviewed RSA cryptosystems and cryptographic scheme, and discusses some security issues and challenges of RSA. The objective of this work is to present holistic appraisal of the RSA cryptosystems.

Keywords
Cryptography, Public-key Cryptosystems, RSA algorithm, Encryption, Decryption, Cryptographic Scheme.

1.0 Introduction

Nowadays, the use of computer has gone beyond their early intentions. They now found use in the e-initiative (e-banking, e–commerce, e–shopping) etc. These phenomenal changes have brought about the need for tight security to data and information as they are transported across network to network[1]. E-banking, e-commerce, e-shopping, etc., transactions over the un-trusted communications channels are now possible because of the application of data encryption mechanisms. The inability to secure data or information where unauthorized access is probable and where other security techniques are inadequate may have necessitated the concept of cryptography.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin [17]. Cryptography is one of the technological means to provide security to data being transmitted on information and communications systems. Cryptography is especially useful in the cases of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over untrusted medium like the Internet [3]. Cryptographic techniques have been providing secrecy of message content for thousands of years [7]. A cryptographic primitive is a basic mathematical operation on which cryptographic schemes can be built [16]. Cryptography is about communication in the presence of adversaries. Cryptographic goals include: privacy/confidentiality, data integrity, authentication, and non-repudiation. A fundamental goal of cryptography is to adequately address these four areas_in both

theory and practice. Cryptography is all about the prevention and detection of cheating and other malicious activities [17]. Cryptography can be applied to safeguard communication channels and physical databases. Cryptography has two techniques: symmetric algorithms (or private key cryptosystems) and asymmetric algorithms (or public key cryptosystems). In the symmetric scheme, the same cryptographic key is used for both enciphering and deciphering processes. Symmetric key do not guarantee security if the sender key is known. In asymmetric cryptographic algorithms, two keys are used: one key, called the public key is used to encrypt the plaintext or message; while the second key, called the private key is used to decrypt the plaintext or message. These two techniques are inherently different from each other.

In the symmetric cryptosystem where the sender and the receiver use the same key, which is kept secret from every one else, the biggest problem is the shared key management. If communications were to take place between you and several people - you need to have different secret keys for each person otherwise each person can read messages meant for one another. The concept of the public key infrastructure conceived by Diffie and Hellman, proffer a solution to get around the problem of key management by using the asymmetric cryptosystem or public-key cryptography. This paper is a review of the public-key cryptography with emphasis on the RSA cryptosystems and cryptographic schemes.

The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography. From its earliest beginnings to modern times, virtually all cryptographic systems have been based on the elementary tools of substitution and permutation [23].

2.0 Public-Key Cryptography

Public-key cryptography is based on the use of a key for encryption and another but related key for decryption. The characteristics of Public-key cryptography are summarized as follows:

- It is computationally difficult to ascertain the decryption key with the knowledge of the encryption key and cryptographic algorithm.
- In some cryptosystems, like RSA, either of the two related keys, e or d, could be used to compute encryption and decryption respectively.

2.0.1 The Essential Steps of Public-Key Cryptography

The essential steps of Public-key cryptography in [23] are:

- Each end system in a network generates a pair of keys to be used for encryption and decryption of messages that it will receive.
- Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.
- If A wishes to send a message to B, it encrypts the message using B's public key.
- When B receives the message, B decrypts it using B's private key. No other recipient can decrypt the message because only B knows B's private key.

2.0.2 Applications of Public-key Cryptography

The use of public-key cryptosystems can be applied to three classes:

- Encryption / decryption: A encrypts a message with B's public-key.
- Digital signature: A "signs" a message with its private key, while for the verification of the signature, only the knowledge of the corresponding public key is necessary.
- Key exchange: This involves two parties agreeing in exchanging a session key. A number of techniques for achieving this abound - with regard knowledge of the private key(s) of one or both parties.

Some algorithms are suitable for all three applications, whereas others can be used only for one or two of these applications [23].

2.0.3 Requirements for Public-Key

Cryptography

The cryptosystem in Table 1 rely on the use of two related keys for its cryptographic protocols. Table 1 shows applications for public-key cryptosystems.

Table 6: Applications for Public-key Cryptosystems [23]

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

2.0.4 Public-key Cryptanalysis

An attacker tries to decrypt encrypted messages using any of the available methods at his/her disposal, such as, brute force – attempts to guess decryption keys; attacks on algorithms and protocol weaknesses, etc.

As with conventional encryption, a public-key encryption scheme is vulnerable to a brute-force attack. The countermeasure is the same: Use large keys. However, there is a trade-off to be considered. Public-key systems depend on the use of some sort of invertible mathematical function. The complexity of calculating these functions may not scale linearly with the number of bits in the key but grow rapidly than that. Thus, the key size must be large enough to make brute-force attack impractical but small enough for practical encryption and decryption. Another form of attack is to find some way to compute the private key given the public key [23].

3.0 Brief History of Asymmetric Cryptosystems And Rsa

The first invention of asymmetric cryptosystems was by James H Ellis, Malcolm Williamson, and Clifford Cocks in the early 1970s. 1976 marked a major breakthrough in the history of asymmetric cryptography. In that year, an asymmetric cryptosystem was published by Diffie Whitfield and Hellman Martin, which came to be known as Diffie-Hellman key exchange, was the first practical method for establishing a shared secret key over an insecure communications channel without bothering on the use of previous shared secret. Cooks method was later reinvented by RSA in 1977 and their work was made published in 1978, and the algorithm came to be known as RSA [28]. The introduction of public-key cryptography by Diffie and Hellman in 1976 was an important watershed in the history of cryptography. The work sparked off interest in the cryptographic research community and soon several public-key schemes were proposed and implemented. The RSA, being the first realisation of this abstract model, is the most widely used public-key scheme today [2]**.** The security of RSA is based on the difficulty of factoring n.

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem [18]. The concept of a digital signature was introduced by Diffie and Hellman. The first practical realization of a digital scheme appeared in the paper in [20].

3.0.1 Review of Cryptographic Scheme

A number of works on the application of cryptographic scheme to secure data from untrusted communications channels based on different computer services and applications have been developed by

academic scholars and researchers over the years. [12] worked on a secure directory service based on exclusive encryption. Their design uses encryption for protecting data privacy and Byzantine replication for protecting data integrity. The context of their work is a secure scalable file system that logically functions as a centralized file service but physically distributed among a network of untrusted desktop workstations.

If across the board services encryption is needed for services like FTP or Telnet, encryption devices are employed. Theses devices examine every network packet before it leaves the private network, and if a packet is destined for outside networks specified by a security administrator, the data portion of the packet is encrypted. Anyone capturing that data packet as it travel over an outside network connection is unable to read it [6]. The blooming e-commerce is demanding better method to protect online user's privacy, especially the credit card information that is widely used in online shopping. Holding all these data in a central database of the web sites would attract hackers' impose unnecessary liability on the merchant web sites, and raises the customers' privacy concerns [11]. The use of encryption techniques is not limited to data and information alone, its use extends to areas where absolute security are needed, such as operating systems, Web applications, GSM, and so on.

Asymmetric encryption algorithm can be used to exchange the key of the

symmetric encryption algorithm because it is t more slowly than symmetric encryption algorithm, so asymmetric encryption algorithm is usually used to secure encryption key of the symmetric encryption algorithm in the practice, but symmetric encryption of message algorithm is usually used to secure the communication [31]. Tamper detection is also accomplished with cryptography technologies [6]. Kerberos is a security protocol developed by MIT. Windows 2000/Active Directory networks use Kerberos to authenticate users logging on to the network. Because Kerberos relies on the asymmetric scheme when exchanging data with the clients and servers involved in the authentication process, all passwords and other sensitive information are always transmitted in encrypted form, and never in cleartext. This ensures that even if an unauthorized individual were to capture the packets exchanged during the authentication procedure, no security compromise would result. Kerberos authentication is based on the exchange of tickets that contain an encrypted password that verifies a user's identity [29]. Cryptographic applications will continue to increase as long as the demand for Internet services continues. All the services provided by the Internet require one form of encryption or another.

The objective of GSM system is to make the system as secure as the public switched network. Radio transmission is the media of transmission for GSM system and this poses a number of threats from eavesdropping. Authentication is used to identify the user to the network operator. It uses a technique that can be described as "Challenge and response", based on encryption. A random challenge is issued to the mobile; the mobile encrypts the challenge using the authentication algorithm (A3) and the key assigned to the mobile, and sends a response back. The operator can check that, given the key of the mobile, response to the challenge is correct [19]. In the GSM System, encryption takes place over the air path.

In the digital world it is easy to impersonate others. Only strong

cryptography can protect against these attacks [21]. The last threat we must guard against is people. People are always the weakest security link. Whether it is a guard being bribed to leave a door open or an unsuspecting employee opening an attachment that turns to be a virus. People are the most difficult security problem. They will forever bypass security they find intrusive, subvert security they find bothersome, and attack the very systems they are supposed to be guarding. On computer networks, inside attacks are much more dangerous that outside hackers. User mistakes are much more damaging than malicious code. It is a problem as old as civilization, and it's not one that computers can magically solve [26].

3.0.2 Review of RSA Cryptosystems

A number of works on the review/modification of RSA cryptosystem have been proposed (or embarked upon) by academic scholars and researchers over the years.

A resemblance of the RSA cryptosystem which uses special kinds of elliptic curves over Z_n, where n is a composite integer, was proposed by Koyama et al. Also, Demytko, presented a resemblance of the RSA cryptosystem where there is very little restriction on the types of elliptic curves that can be used. A new cryptosystem based on elliptic curves over Z_n in which the message is held in the exponent instead of the group element was proposed by Vanstone and Zuccherato. The security of all these schemes is based on the difficulty of factoring n [18].

Rabin encryption scheme is a modification of the RSA cryptosystem where cryptograms are generated using the fixed public key k = 2, and $C = M^2$ (Mod N), where N is the modulus. A legal recipient, who knows the proper factorizing of N, can decrypt by computing two congruences, in Z_p and in Z_q, respectively, using the Chinese Remainder Theorem. Rabin's cryptosystem has the disadvantage that its encryption process is not one-to-one for all messages. There is 4:1 ambiguity in the decrypted message [22]. Williams presented a public-key encryption scheme similar to Rabin's but using composite integer n = pq with primes p ≡ 3 (mod 8) and q ≡ 7(mod 8). Williams' scheme also has the property that breaking it is equivalent to factoring n, but has the advantage over Rabin's scheme that there is an easy procedure for identifying the intended message from the four roots of a quadratic polynomial. However, a further work by Williams later removed the restrictions on the forms of the primes p and q [18].

Williams showed how to redefine Rabin's scheme to overcome most of the drawbacks. He has proved that the decryption process can be simplified for all messages M whose Jacobi symbol is: $\left(\frac{M}{N}\right)=1$

Where, primes are selected in such a way that:

P = -1(mod 4) and q = -1(mod 4), then the deciphering process is expressed by the following congruence:

$$C^k = \pm M(\text{mod } N)$$

Where, the secret key k = 1/2[1/4(p – 1)(q – 1) + 1]. In Williams' scheme, the receiver selects N using p = -1(mod 4) and q = -1 (mod 4) and a small integer S such that $\left[\frac{S}{N}\right]=-1.$ and publish N and S but keeps secret the key k [22]. William's further considered the cryptosystem where cryptograms are generated using the fixed public key k = 3, and $C = M^3$ (Mod N), where N is the modulus. He was able to show and proved that it is as difficult to break as it is to factor N.

Another modification of the basic RSA system for k ≡ 3 (modulus 18) have been presented by Khoo, Bird and Seberry. However, they recommended that their modification should be used for k, whose binary representation has several zeros. Their work is defined in the ring $Z(\omega)$ where ω is a primitive cube root. They also proved that it is as difficult to break as it is to factor N.

In RSA scheme, p and q should be almost the same bit lengths. Shamir proposed a variant of the RSA encryption scheme called unbalanced RSA, which makes it possible to enhance security by increasing the modulus size (e.g. from 500 bits to 5000 bits) without any deterioration in performance. In this variant, the public modulus n is the product of two primes p and q, where one prime (say q) is significantly larger in size than the other; plaintext messages m are in the interval (0, p-1) [18]. The computational equivalence of computing the secret key d, and factoring n was shown by Rivest, Shamir and Adleman, based on earlier work by Miller [18].

A system is computationally secure if the task of inverting the plaintext is computationally infeasible or traceable [22]. A trapdoor in the RSA cryptosystem was proposed by Anderson, whereby a hardware device generates the RSA modulus n = pq in such a way that the hardware manufacturer can easily factor n, but factoring n remains difficult for all other parties. However, Kaliski subsequently showed how to efficiently detect such trapdoors and, in some cases, to actually factor the modulus [18]. A number of works has been put forward by eminent scholars in the area of email security. The scope of their researches covers the same territory but with some differences in approach and technology.

An example of the use of cryptography in this regard is the PGP – Pretty Good Privacy scheme proposed for adding privacy to Internet mail applications. PGP was invented by Phil Zimmermann to provide all four aspects of security (Privacy, integrity, authentication and nonrepudation) in the sending of email [13]. PGP encrypts data by using a block cipher called IDEA (International Data Encryption Algorithm). It takes plaintext as input and produces signed cipher-text in base64 as output. The sender starts by invoking the PGP program on his/her computer. PGP first hashes the message using MD5, and then encrypts the resulting hash using his/her private RSA key. When the receiver gets the message, he/she can decrypt the hash with the public key of the sender and verify that the hash is correct. Even if someone else could acquire the hash at this stage and decrypt it with the sender's known public key, the strength of MD5 (Message Digest) algorithm guarantees that it would be computationally infeasible to produce another message with the same MD5 hash [24].

Like PEM, PGP generates and manages secret keys on behalf of a user and uses asymmetric encryption only to transmit secret keys to the intended communication partner. PEM uses both public and secret-key encryption - mail users obtain a public/private key pair from a local PEM program and publish the public key with their mail address. Each user relies on a local PEM program that maintains a small database of their keys. The PEM is available as an application program called RIPEM that uses a public-key encryption library called RSAREF produced by RSA Data Security Inc, under license from PKP (public key partners), a firm that owns a patent covering the RSA public key encryption method [8]. In [1] any

cryptosystems, two fundamental assumptions are made as follows:
(i) The cryptanalyst (the intruder) knows the encryption algorithm;
(ii) The medium of transmission is insecure.

3.0.3 Cipher

A cipher is a character-for-character or bit-for-bit manipulation irrespective of the language structure of the message/data. In other words, a cipher is an algorithm for executing encryption and decryption. The following are some major ciphers: substitution, transposition, block and stream.

Substitution Cipher

Substitution cipher is when a letter or a collection of letters is replaced by another letter or collection of letters with the aim of scrambling it, usually in a preserved order of the plaintext.

Transposition Cipher

Transposition cipher maintains the characters of the plaintext but reorders its position to create the ciphertext. The text is structured into a matrix form whose columns are interchanged using a key. The substitution and transposition cipher are traditional ciphers.

Block cipher

Modern ciphers employ the use of block and stream ciphers. In block cipher, the unit of encryption/decryption is based on a block of bits.

A block cipher is an encryption scheme which breaks up the plaintext messages to be transmitted into strings (called blocks) of a fixed length t over an alphabet A, and encrypts one at a time [18].

- **Stream Ciphers**

Stream ciphers can be viewed as a block cipher with a block length equal to one. For any encryption transformation there must be change for each symbol of plaintext. Stream ciphers are useful where transmission errors are highly required because they do not propel errors. Stream ciphers are useful when plaintext must be encrypted one symbol at a time.

3.0.4 Encryption and Decryption

Encryption and decryption are the algorithms used for manipulating cryptographic schemes.

Encryption

Encryption or enciphering is the scrambling of data/messages in some way to make it unreadable.

Decryption

Decryption or deciphering is the unscrambling of data/messages in some way to make it readable. Decryption or deciphering is possible with keys that are related. A message read/sent across a network or communication channel is referred to as the plaintext whereas the encrypted message is the ciphertext.

Although, the transformation of encryption and decryption is the inverse, the private key system handles the data as a bit, but the public key system handles the data as a number that perform function operation and the mathematical function is one-way. It is to say, it can easily come true from one side, but very difficult to another side, so simple steps unable to decrypt the cipher text [27].

3.0.5 Components of Cryptography

Cryptography has three major components: cryptosystems, protocols and key management.

Cryptosystems

Cryptosystems is considered to be the collection of encryption and decryption systems, the key generator, as well as the protocols for key transmission [22]. The term cryptosystems is used to describe cryptographic algorithms and their characteristics.

Cryptographic Protocols

The term cryptographic Protocols, is used to describe the composition and application of cryptographic algorithms with regards to securing of a communications channel or information in a database.

A protocol is a series of steps taken to accomplish a task. In fact that is also the definition of an algorithm but we use algorithm to refer to the attainment of internal, mathematical results like encrypting a block, and protocol to refer to the attainment of user-visible results such as secret communication and digital signatures [25]. A Protocol is a set of rules and conventions that defines the communication framework between two or more agents. These agents, known as principals, can be end-users, processes or computing systems. Security related and cryptographic protocols are used to establish secure communication over insecure open network and distributed system. These protocols use cryptographic techniques to achieve a specific security objective. Unfortunately, open networks and distributed systems are vulnerable to hostile intruders who may try to subvert the protocol design goals [14].

Key Management

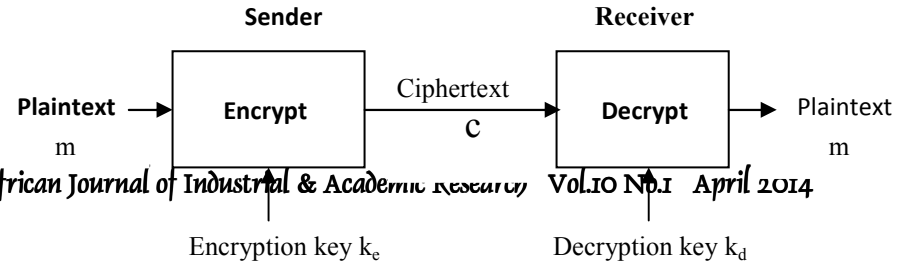
The term key management is used to refer to the fundamental problems of creating, distributing, and storing keys.

4.0 Cryptographic Algorithms

A cryptographic algorithm is defined to be the mathematical description of the enciphering and deciphering processes together with the interrelation between their keys. Cryptographic algorithm is more software oriented [22].

4.0.1 Asymmetric Cryptosystems

Asymmetric cryptosystems involves two keys – a private key and a public key that are mathematically related. A message encrypted with one key can be decrypted only with the other. It is extremely difficulty to determine the value of one key by examining the other. In an asymmetric cryptosystem, the encryption key is different from the decryption key. The public key is often called the encryption key. Figure 1 shows an asymmetric cryptosystem. Typically, each participant in public key cryptosystem creates his own key pair. Then one member of the pair, called the private key, is kept secret never revealed to anyone else, whereas the other member of the key part, called the public key is distributed freely. Either key may be used for encryption or for decryption, but the most important point is that the private key never be revealed.



4.0.2 Functions of Asymmetric Cryptography

Asymmetric cryptography provides the following functions: privacy, authentication, integrity, and nonrepudiation A fundamental goal of cryptography is to adequately address these four functions in both theory and practice.

Privacy

Privacy is a secret message whose contents are known only by the sender and receiver. The recipient public key is used to encrypt the message and with the secret key in his possession, he can decrypt the message.

1.

2.

Authentication **3.**

Authentication arises when the receiver knows who sent the message and its genuineness and the sender knows that the message shall get to the intended recipient. The recipient has the ability to authenticate the sender of the message by simply verifying a digital signature.

Integrity

Integrity arises when the receiver knows that the message was not corrupted or modified either deliberately or accidentally while in transit. Digital signature message offers message integrity. The encryption of the message is done with the sender's private key.

Nonrepudiation

The sender of the message cannot reject that the message did not originate from him/her. In asymmetric cryptography, the provision of nonrepudiation is possible using digital signatures. An attack may have an adverse effect on one, or a combination of all these functions [15].

5.0 THE RSA ALGORITHM

The RSA scheme is a block cipher in which the plaintext and the ciphertext are integers between 0 and n-1 for some n [23].

1.0 THE RSA ALGORITHM

The RSA scheme is a block cipher in which the plaintext and the ciphertext are integers between 0 and n-1 for some n [23].

RSA Algorithms for Secret Communication

RSA algorithms for privacy for the existing system include: algorithm for key generation and algorithm for asymmetric encryption.

Algorithm for Key Generation

If communication must exist between two entities, X and Y, each entity must be capable of creating an RSA public key and a related private key. X follows the procedure as follows:

(a) Generate any two large prime numbers, p and q having approximately the same size.

(b) Compute n = pq and z = (p-1) (q-1).

(c) Compute public key, e, by choosing any number that is relatively, prime with z such that e has no common factors with z.

(d) Compute private key, d, by solving the equation: e x d = 1 (mod z).

(e) X's public key is (n, e) and X's private key is d. e, d are the encryption and decryption exponents, n is the modulus.

Algorithm for RSA Asymmetric Encryption

Y encrypts a plaintext m meant for X, and X decrypts it. Y follows the procedure in (a) and Y follows the procedure in (b):

(a) Encryption:

1. Get X's public key, (n, e).

Prepare the plaintext for computation in the interval, [0, n-1].

3. Compute $c = m^e \bmod n$.
4. Send encrypted text or cipher text c to X.

(b) Decryption:

X uses the private key, d, to compute:

$m = c^d \bmod n$ (to recover message m).

Where:

m is the original Message/Plaintext.
c is the Cipher text/ encrypted text.
e is the Encryption key.
d is the Decryption key.
n is the RSA modulus.

4. RSA Algorithm for Digital Signatures

RSA algorithms for digital signatures for the old system include: key generation, signature generation and verification. Algorithm for Key Generation is the same as in RSA algorithms for Secret Communication.

Algorithm for RSA Signature Generation and Verification

In a Digital Signature scheme, X can sign a plaintext $m \in M$. Y is capable of verifying X's signature and recover the plaintext m from the signature.

(a) **Signature Generations:**

To sign a message_ X follows the procedure as follows:

1. Compute $m = D(m)$.
2. Compute $s = m^d \bmod n$.
3. X's signature for the message, m is s.

(b) **Verification:**

Y can verify X's signature s and recovers the message m as follows:

1. Get X's public key (n, e).
2. Calculate $m = s^e \bmod n$.
3. Verify if $m \in M_D$ otherwise rejects Signature.
4. Compute $m = D^{-1}(m)$ to recover the message.

D is the redundancy function $D:M \; Z_n$, $(D(m) = m$ for all $m \in M)$, s is the signature, M is the result of the redundancy function.

5.0.1 Secret Communication and Digital Signatures

Secret communication and digital signatures are cryptographic protocols. Protocols use cryptographic schemes to achieve a specific security objective. Protocols play a major role in cryptography and are essential in meeting cryptographic goals. Encryption schemes and digital signatures are some examples of protocols.

Secret Communication

Secret communication is a situation whereby a message is made secrete and only the sender and intended recipient knows the contents of the message.

Asymmetric Encryption

Asymmetric encryption is a secrete communication where a message is encrypted using the recipient's public key and only the intended recipient has the rightful private key to decrypt the message – it is known as privacy. Figure 2 shows an illustration of secure communication service for asymmetric cryptosystem.

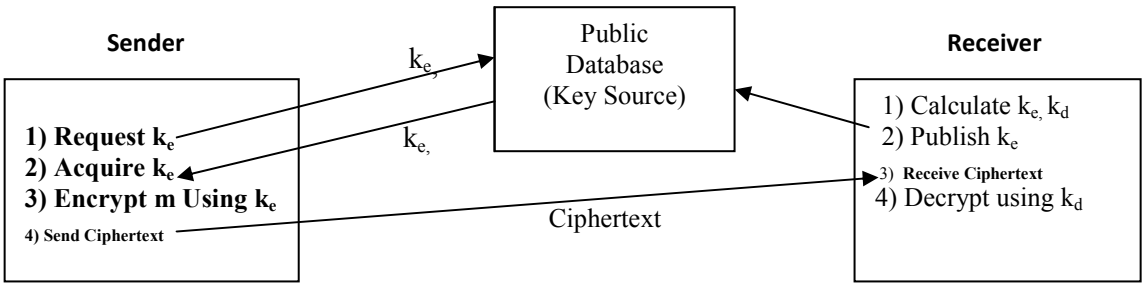


Fig. 2: Illustration of secure communication service for asymmetric cryptosystem

3. Digital Signatures

The concept of digital signature is not a new phenomenon. Digital signature was introduced by Diffie W. and Hellman M, over three decades ago in [10]. In asymmetric cryptosystems, we can achieve the following basic form of security: authentication, integrity, and nonrepudiation by using what is called digital signature.

A digital signature scheme is a public key algorithm that allows one to authenticate a message by means of a piece of information called the signature. The generation of the signature requires the knowledge of the signer's private key, while for the verification of the signature, only the knowledge of the corresponding public key is necessary. If the public key is publicly accessible, then everybody can verify the signature, while only the signer, who known the private key, is able to sign. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information**.** Figure 3 shows an illustration of digital signature using asymmetric cryptosystems

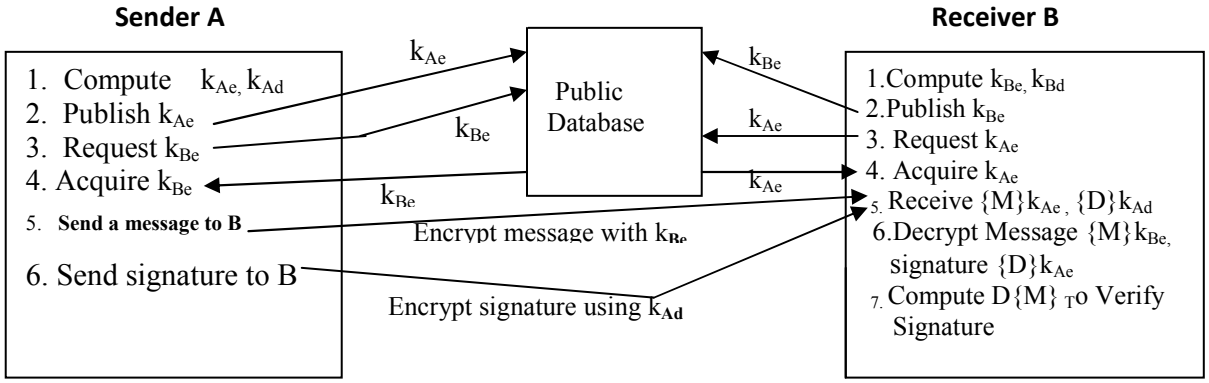


Fig. 3: Illustration of digital signature using asymmetric cryptosystems

6.0 The Security Of Rsa And Challenges

The security of RSA according to [23], has three possible approaches to attacking the RSA algorithm, these are stated as follows:

Brute-force: This involves trying all possible private keys

Mathematical attack: There are several approaches, all equivalent in effect to factoring the product of two primes.

Timing attacks

These depend on the running time of the decryption algorithm The system structure of

RSA algorithm is based on the number theory of the ruler. It is the most security system in the key systems. The safe of RSA algorithm bases on difficulty in the factorization of the larger numbers [30]. As a matter of fact, implementing high-security RSA on embedded systems is nowadays a difficult technological challenge, despite the steady hardware developments of the last years. Indeed, an important requirement for a practical cryptosystem is its speed. Whereas for specific applications a highly secure, yet slow cryptosystems can be used, for a general deployment a system must make reasonable use of the available resources such as memory, speed, bandwidth [5]. If any of the two prime factors of a participant's public RSA-modulus can be found, then the private key of that participant can be found, and the system is considered to be broken. If the primes are properly chosen (that is large enough), then finding them given only their product (the RSA-modulus) is believed to be a computationally infeasible task. To make the system secure the primes must therefore be chosen sufficiently large. On the other hand, large primes imply a large RSA-modulus, which leads to substantial computational overhead when using the RSA system. Thus, in RSA there is a trade-off between security and efficiency: on the one hand moduli must be large for security; on the other hand small moduli are preferred for efficiency. How large they have to be, depends on the speed of socalled factorization algorithm [9].

7.0 Conclusion

In this study, we did a comprehensive review of public-key cryptosystems in general and RSA algorithm in particular. We found out that on the whole, the RSA algorithm is a good algorithm but its implementation has some challenges. One of such is the low speed of encryption and decryption compared with the symmetric cryptographic algorithm. The RSA cryptosystems relies on the difficulty of factoring very large numbers and if there is an algorithm that can decompose a large number fast, the RSA algorithm's security would be threatened.

The defence against the brute-force approach is the same for RSA as for other cryptosystems – namely, use a large key space. Thus, the larger the number of bits in e and d the better. However, because the calculation involved, both in key generation and in encryption/decryption, are complex, the larger the size of the key, the slower the system will run [23]. The RSA system has been shown to provide less security than initially believed. Still, RSA has remained unchallenged among the public key cryptosystems in terms of dissemination. [5]. Virtually all the major types of cryptography in use today rely on the use of one-way functions, mathematical functions that are easy to compute but impractical to invert, or reverse. For example, it is easy to multiply together two large prime numbers, but it is computationally impractical to reverse that by factoring the resulting product. That is the basis of RSA cryptography. Similarly, it is easy to compute $a = x^n$ given x and n, but hard to compute the discrete logarithm n given a and x.

The "discrete logarithm problem" is the basis for a number of cryptosystems, such as the Diffie-Hellman protocol and elliptic curve cryptography [4]."In the 21st century, even the most secure isolated systems have been penetrated [32].With the year-on-year increase of the amount of data and the continuous improvement of people's needs, RSA faces various challenges, application security, data security and privacy, cloud security, denial of service attacks, Advanced Persistent Threats (APTs), mobile security and so on. There are the prospects of the development in the few years [33].

References

[1] Adewumi, S. E., Garba, E. J. D., (2002), Data Security: A Cryptosystems Algorithm Using Data Compression and Systems of Non-Linear Equations, COMPUTER Association of Nigeria Conference Series, Volume 13, 200-221.

[2] Alese, B. K., Philemon, E. D., Falaki, S. O. (2012), Comparative Analysis of Public-Key Encryption Schemes, International Journal of Engineering and Technology Vol. 2, No. 9, Sept., pp. 1552 – 1568.

[3] Almarini, A. and Alsahdi, U. (2012), Developing a Cryptosystem for XML Documents, International Journal of Information Science, Vol. 2. No. 5, pp. 65 – 69.

[4] Anthes, G. (2014), French Team Invents Faster Code-Breaking Algorithm, Communications of the ACM, Vol. 57 No. 1, Pages 21-23, **http://cacm.acm.org/magazines/2014/1/170850-french-team-invents-faster-code-breaking-algori, accessed Feb. 2014.**

[5] Avanzi, R., Ockle, G. B., Braeken, A., Cid, C., Geissler, K., Granger, R., Lange, T., Lenstra, A. K., Nguyen, P. Q., Preneel, B., Sendrier, N., Smart, N. P., Stam, M., Stern, J., Wolf, C. (2005), Alternatives to RSA (Lightweight Asymmetric Cryptography and Alternatives to RSA), The IST program under Contract IST-2002-507932,

[6] Avolio, M. F., (1994), Network Security: Building Internetwork Firewalls, Business Communications Review January (http://www.avolio.com)

[7] Chaum, D. (1981), Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM Feb. 1981 volume 24, No. 2, 1-9, (http://world.std.com/crypto./chaum-acm-1981.html)

[8] Coulouris, G., Dollimore J., and Kindberg T. (1994), Distributed systems, Concepts and Design, Addison-Wesley Publishing Company, USA., Second Edition, 490 - 492.

[9] De, S. Haldar, A., and Biswas, S. (2013), A Review on Recent Trends in Cryptography, International Journal of Latest Research in Engineering and Computer (IJLREC), Vol.1, Issue 1.Sept- Oct., pp. 50-55.

[10] Diffie, W, and Hellman, M., (1976), New Directions in Cryptography, IEEE Trans, Info. Theory, 644-654.

[11] Donghua, X., Chenghnuai, L., and Andre, D. S., (2002), Protecting Web Usages of Credit Cards using One-Time Pad Cookie Encryption, IEEE computer society, proceeding the 18th Annual Computer Security Applications Conference (ACSAC'02).

[12] Douceur, R. J., Adya, A., Benaloh, J., Bolosky, J. W., and Yuval, G., (2002), A secure Directory Service based on Exclusive Encryption, IEEE Computer Society, Proceeding of the 18th Annual Computer Security Application Conference (ACSAC'02).

[13] Forouzan, A. B. and Fegan, S. C., (2004), Data Communication and Networks, Tata McGraw-Hill Publishing Coy Limited, New Delhi, Third Edition, 848 - 849.

[14] Gritzalis S., Spinellis D., Georgiadis P., (1999): Security Protocols Over Open Networks and Distributed Systems: Formal Methods for their Analysis, Design, and Verification, Computer Communications 22 (8); May, 695-707.

[15] Haggerty, J., Shi Q., Merabti M., (2002), **B**eyond the Perimeter: The Need for Early Detection of Denial of Service Attacks, IEEE Computer Society, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02).

[16] Huang, Y., Rine, D., and Wang, X., (2001), A JCA-based Implementation Framework for Threshold Cryptography, IEEE Computer Society, Proceedings of the 17th Annual Computer Security Conference (ACSAC'01).

[17] Menezes, A., Oorschot, P. V., and Vanstone S., (1996), Handbook of Applied cryptography,

CRC Press Inc, (Http//:www. cacr.math.uwaterloo.ca/hac

[18] Menezes, A, Oorschot, P. V. and Vanstone S., (1997), Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC press.

[19] Oyeyinka, I. and Obianyo-Agu N., (2002), Security and Encryption Techniques in the GSM NETWORKS, COMPUTER Association of Nigeria Conference Series, Volume 13, 136-142.

[20] Rivest, R. L., Shamir, A., and Adleman, L., (1978), A Method for Obtaining Digital Signature and Public-key Cryptosystems, Communications of the ACM, Feb., 21:120-126.

[21] Schneier, B., (1997), Why Cryptography is Hard that it looks, Counterpane Internet Security Inc., 1- 4, (http://www.schneier.com/essay-037.html.).

[22] Seberry, J. and Pieprzyk, J., (1998), Cryptography: An Introduction to Computer Security, Prentice Hall of Australia Pty Ltd.

[23] Stalling, W. (1999), Cryptography and Network Security: Principles and Practice, 2nd (Ed.), Printice-Hall Inc., New Jersey, USA, Pp. 163-182.

[24] Tanenbaum A. S., (2005): Computer Networks, Prentice-Hall of India Private Limited, New Delhi, Fourth Edition, 799-804.

[25] Treese G. W., and Stewart C. L., (1998), Designing Systems for Internet Commerce, Addison Wesley Coy.

[26] Walsh, M. L. (2003), Moving Beyond, Information Security, Sept., 1-96.

[27] Wang, H. and Song, R. (2011). The length of the key influences the degree of security of the RSA system. Comput. Knowledge Technol., 10: 7104-7105.

[28] Wikipedia, Public-key Cryptography, the free encylclopedia, http://en.wikipedia.org/wiki/secure computing, accessed May, 2012.

[29] Zacker, C. (2001): Networking: The Complete Reference, Osborne/McGraw-Hill, USA.

[30] Zhang, Y. and Cao, T. (2011). Application of encryption based on RSA algorithm. Sci. Technol. Advisory (Technol. Admin.), 25: 79-80.

[31] Chen, C. and Zhu, Z. (2006). Application of RSA algorithm and implementation details. Comput. Eng. Sci., 9: 13-14.

[32] Kerner, S. M. (2013), RSA 2013: Is Cryptography Still Necessary? **http://www.esecurityplanet.com/network-security/rsa-2013-is-cryptography-still-necessary.html**, accessed Feb. 2014.

[33] N**a**Qi, Wei Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen, Xiaoyan Yin, Xiangrong Xiao and Jie Hu, (2013). Analysis and Research of the RSA Algorithm. *Information Technology Journal, 12: 1818-1824,* **DOI:** 10.3923/itj.2013.1818.1824, **http://scialert.net/abstract/?doi=itj.2013.1818.1824,** accessed Feb. 2014.

Enhancing Image Retrieval System Using Content Based Search Criteria

[1]Umoh E. E, and [2]Mbam, B. C. E

[1]Department of Computer Science , Cross River University of Technology, Calabar,
Tel: 08037134736, e-mail: enoimah@yahoo.com.
[2] Department of Computer Science, University of Agriculture, Umudike,
Tel: 07036597010, e-mail: quicksuccessng@yahoo.com.

Abstract

The purpose of this work is to design and implement a software that enhances the retrieval of image using the image content base as the criteria. As the size of multimedia databases and other repositories continues to grow, the difficulty of finding multimedia information increases, it becomes practically impossible to depend on the metadata of images for retrieval. Therefore, the development of a content-based image retrieval system becomes necessary to structure the retrieval of an image by its content. This work provides a good alternative to the normal retrieval pattern by making use of a browser that would search and retrieve image based on content. For fast retrieval of images the user must provide the appropriate parameters required for the retrieval, such as image category, extension format, color and dimension (width and height) of an image. The output shows more efficiency in retrieval because instead of performing the search on the entire image database, the image category option directs the retrieval engine to the specified category. Also, there is provision to update or modify the different image categories in the image database as need arise.

Keywords: *Content-based, Multimedia, Search Engine, Image-based, Texture, Query.*

Introduction

The use of images in human communication in our contemporary society is in very high demand. Images now play a crucial role in fields as diverse as medicine, journalism, advertising, education and entertainment. Technology in the form of inventions such as photography and television has played a major role in facilitating the capture and communication of image data [2]. However, the real engine of the image revolution has been the computer. The involvement of computers in imaging can be dated back to 1965, with Ivan Sutherland's sketchpad project, which demonstrated the feasibility of computerized creation, manipulation and storage of images, though the high cost of hardware limited their use until the mid 1980s [1].

Once computerized or digitized images became affordable, largely the development of a mass market for computer games, it soon penetrated into areas traditionally depending heavily on images for communication, such as engineering, architecture and medicine. Photography libraries, art galleries and museums, too began to see the advantages of making their collection available in electronic form [6].

The image is content-based means that the actual content of the image might be referred to colors, textures, shapes and other information that can be derived from the image itself rather than the metadata such as

tags, descriptions or keywords associated with the image [4]. Therefore, content-based image retrieval system is desirable taking into consideration the quantity and quality of the image.

Retrieving images using content-based retrieval system could be problematic because;

1. The retrieval of image and other multimedia data is quite different from the method used for conventional documents.
2. Its key technique is having the ability to automatically derive image features, such as color, texture, shape, width and height.
3. Most of the web search engines rely purely on metadata and this produces a lot of garbage results.

Therefore, an efficient and effective tool that can retrieve images based on its content keeping track of the content and quality of the image is very essential. With the considerable potential that content-based image retrieval holds as a fast growing technology, it is necessary that the way and manner in which images are retrieved does not pose any problem to the user [5]. Also, there is need to automatically regulate the image search engine.

Therefore, there is need to develop a browser or search engine that can effectively and efficiently retrieve image based on its content and metadata by specifying the width, height and color for easy retrieval. User queries must match when retrieving an image.

This has become imperative due to the fast development of digital cameras and computer technology, where large number of images are collected and stored in computers and other digital devices. Systematic management of these image data is therefore very important for future use and applications.

In his work "Development of a perception oriented texture-based image retrieval system for Wallpapers" [8], there are two approaches commonly used, one is text-based image retrieval and the other is content-based image retrieval.

Today, image digitization, compression and archival has become popular and inexpensive, straight forward and there is broad range of available hardware and software to support these tasks [3].

Methodology

The proposed system is a search engine that will search for images using content-based search criteria such as color and dimensions of the image. The search engine will combine similarity measures, semantics and content-based information in the retrieval of relevant search results that satisfy the user's query. It will operate by accepting queries from it users through the search criteria. Now, Depending on the type of image and its features that have been specified, a connection is established to the database and the search commences.

Using similarity measures, the content-based and multidimensional feature vector applied on relevant images are retrieved and the searches which are more similar to the user's query are displayed [7].

Requirements

Input Requirement: The input requirement will consist of a graphic interface that will enable the users to query by providing the search criteria such as dimension and color chosen from a listbox. These also include access to the application and other options to implement the software.

Output Requirement: The output requirement consists of a window to display the collection of image category in thumbnails. Each of the images displayed contains a link that displays a collection of images under it. The first display is known as image category, while the sub-images of the image category are known as the image collection.

Database

The database design is the creation of a conceptual model of a database that is structured for the insertion and retrieval of images. This consists of the image retrieval table and the image insertion table.

Table 1.1: Photo.

Column Name	Data Type	Allow Null
Photo_Id	Int	No
ImageCategory_Id	Int	Yes
Filepath	Varchar(30)	Yes
Extension	Varchar(50)	Yes
Color	Varchar(50)	Yes
Width	Varchar(50)	Yes
Height	Varchar(50)	Yes
Name	Varchar(50)	Yes

Table 1.2: Photo Collection

Column Name	Data Type	Allow Null
Id	Int	No
Photo_Id	Int	Yes
Photo	Varchar(50)	Yes

System Data Flow Diagram

This shows a breakdown of the program modules and describes in details the information flow of the system. It considers the required information for the implementation of the modules describe in the high level diagram. For the purpose of this work we shall limit our system function to the data flow diagram only.

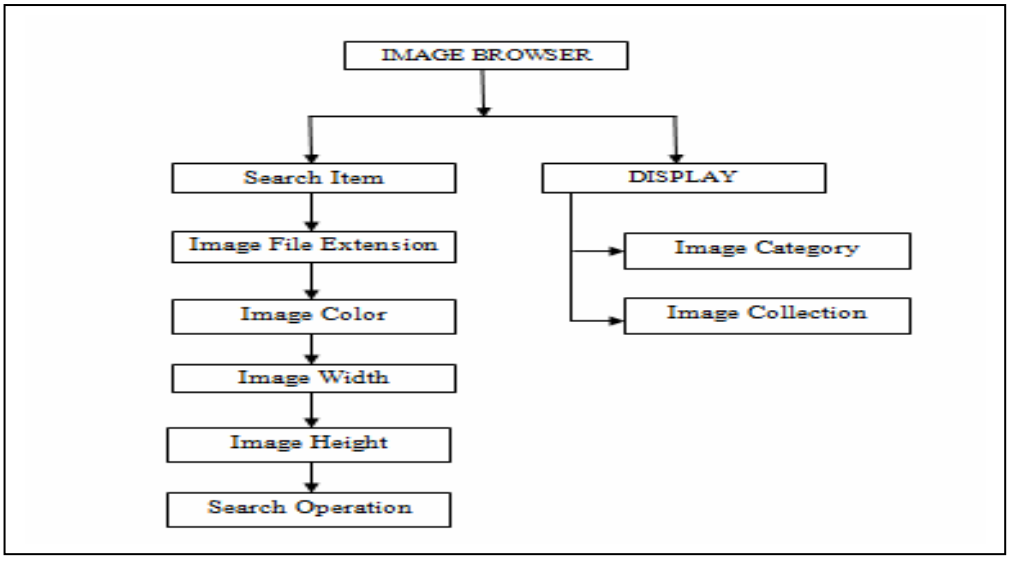


Figure 1.1: Data Flow Diagram

Program Flowchart

There are three basic flow charts: User flowchart, image category flowchart and the image collection flowchart.

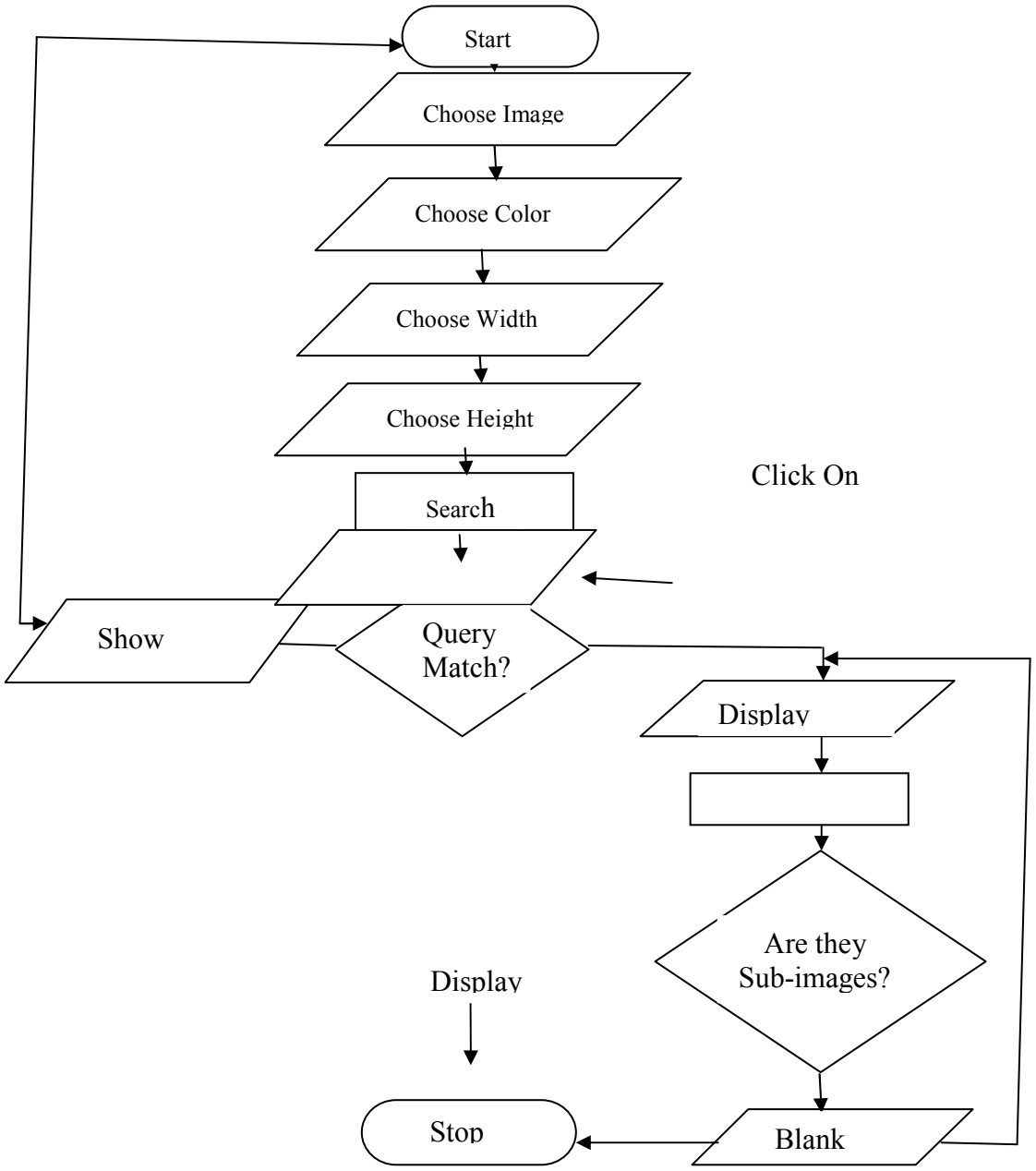


Figure 1.2: User Flowchart

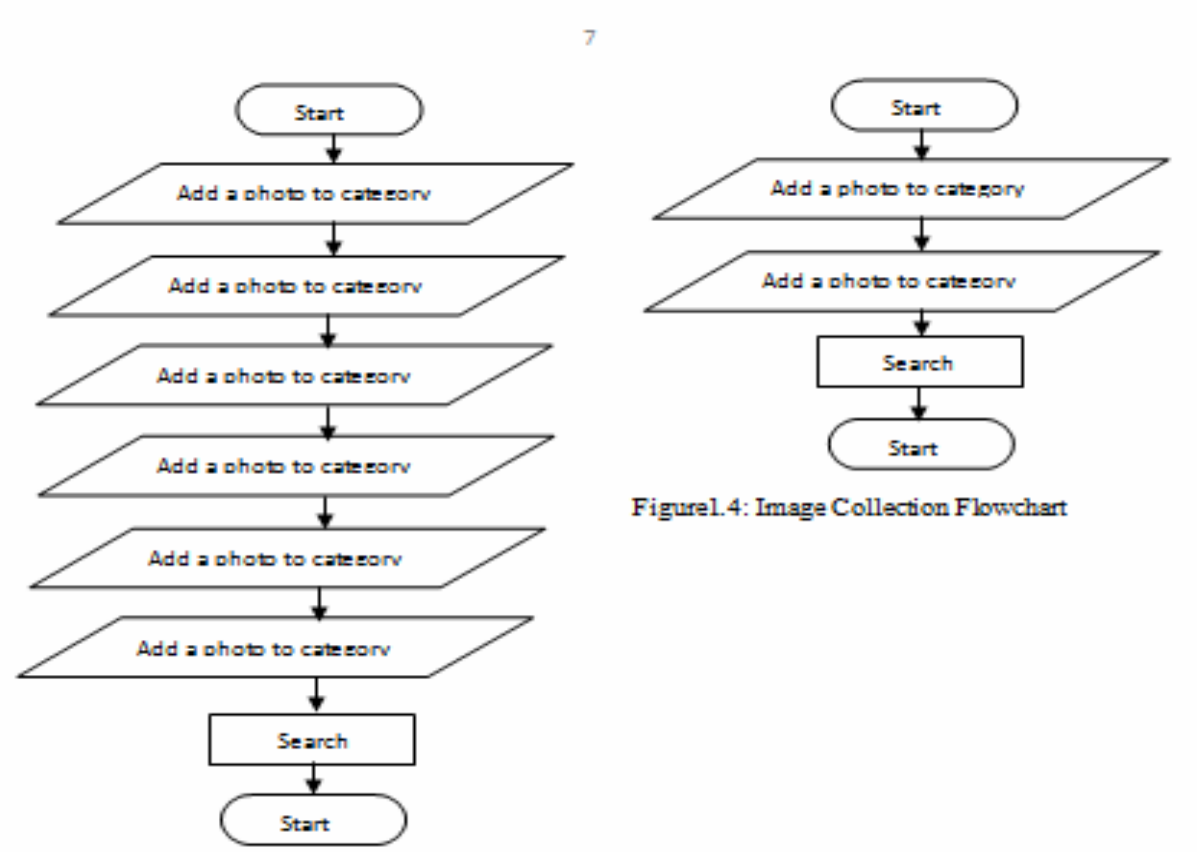


Figure1.4: Image Collection Flowchart

Figure 1.3: Image Category Flowchart

System Design and Implementation

The image search engine is a single interface application with other procedures that brings out the complete functionality of the application. The system components of the search engine are as listed below:

i. arch item combo box
ii. Extension textbox
iii. Width textbox
iv. Height textbox
v. Color textbox
vi. Search button
vii. Display area

The input required for the execution of the content-based image retrieval system is a query to the file extension of the image, color of the image, width and height of the image. All these attributes describe the relationship with the image search engine and what the user require.

Discussion of the Result

The main idea has been to structure the retrieval system of an image by it content. The retrieval method uses the criteria that are pertaining to a particular image as it can be identified by professionals in the field. The content is searched and retrieved with improved retrieval efficiency. What makes it more efficient is that instead of performing the search on the entire image database, the image category option directs the retrieval engine to the specified category, such as sports, automobile, game, and so on. What is important here is the regular update of the image category database. See figures below:

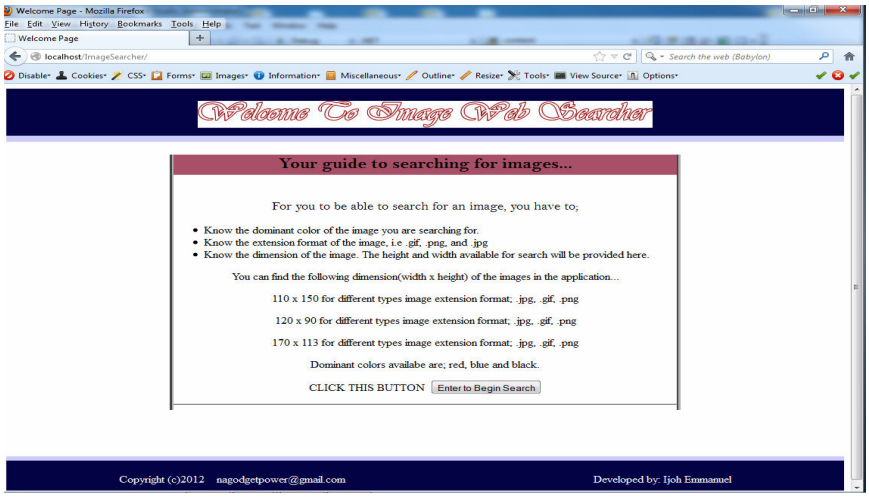


Fig. **2.1: Graphic User Interface showing the options to proceed or exit the program.**

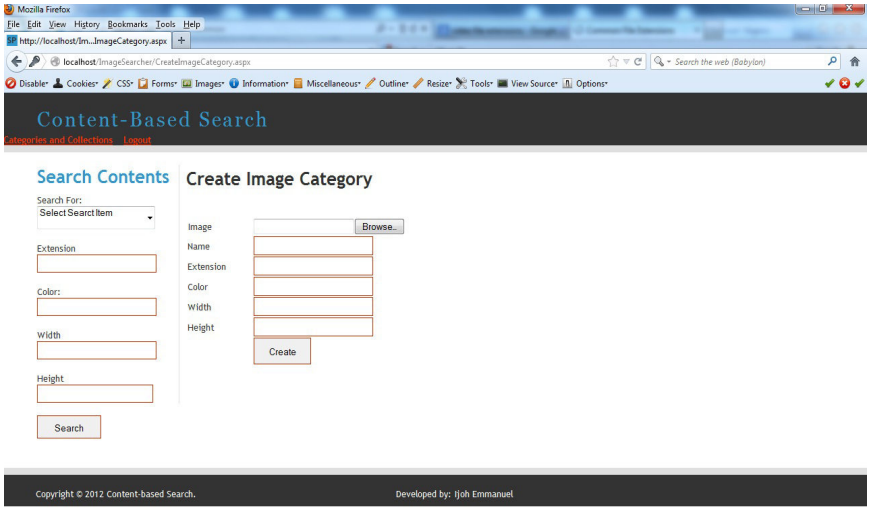


Fig. 2.2: Image Categorization Screen

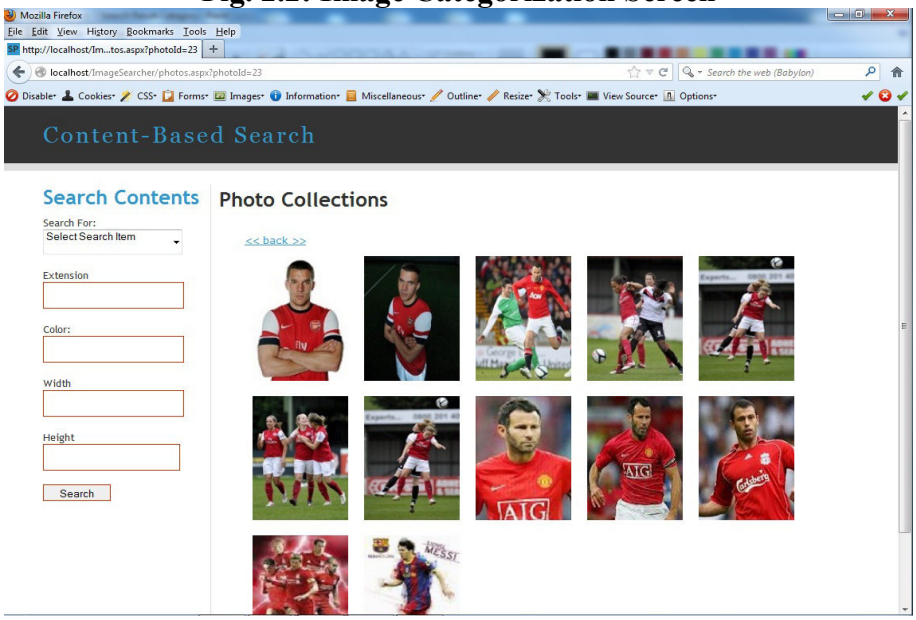


Fig. 2.3: Image Collection Screen to add photo to the collections

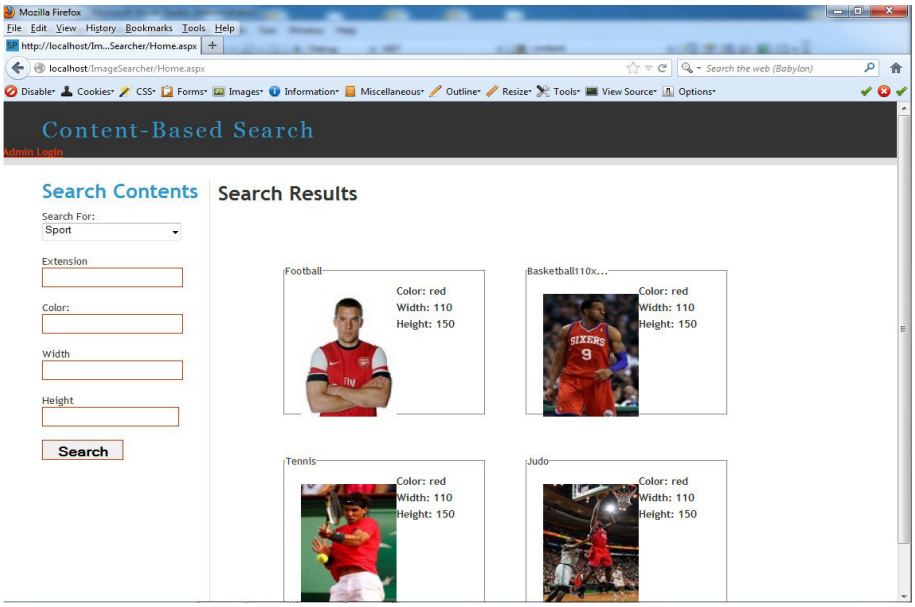


Fig. 2.4: Search result.

Notice that the result displayed indicates the parameters of the image as used in the search criteria, that is, the color, width and height of the image.

Conclusion

The main idea has been to offer a solution that will improve the results of searching for image. It could be from storage media or on the internet. The development of a content-based image retrieval system becomes necessary to structure the retrieval of an image by its content. Using the content criteria therefore provides an improved method that enhances the retrieval efficiency of image retrieval systems. It also provide a good alternative to the conventional retrieval pattern by making use search engine or browser that would search and retrieve images based on it contents.

References

[1] Datta, R., John, D., and Wang, A. J. (2008). Image Retrieval: Ideas, Influences and Trends of the New Age, Michael West Publishers, USA.

[2] Gaurav, Jaswal, Kaul A. (2000). Content-based Image Retrieval – A Literature Review. National Institute of Technology, Hamirpur, India.

[3] Jerry, Z., Hallquist, A., Liang, E. (2002). Image-based Localization. (http://google.com) 26th May, 2013 at 4.00pm.

[4] John, E., and Graham, M. (2000). Content-based Image Retrieval, University of Northumbria, Newcastle.

[5] Remco, C. V., and Tanase, M. (2000). Content-based Image Retrieval System: A Survey (http://google.com), 13th June 2013 at 2.00pm.

[6] Stan, S., Taycher, L., and Cascia, M. L. (2005). Image Rover: A Content-based Image Browser and Image Digestion for the World Wide Web.

[7] Van den Broek, F. L., Kister, P. M. F., and Vuupijl, L. G. (2004). The Utilization of Human Color Categorization for Content-based Image Retrieval, San Jose, CA.

[8] Yu Qian (2008). Development of a Perception Oriented Texture-based Image Retrieval System for Wallpapers, USA.

The Increasing Complexity of Hacker Attacks on Personal and Corporate Information Systems: A Proactive Mitigation Response Model

[1]Osuagwu O.E., [2]Ndigwe Chinwe, [3]Ijeoma Agwamba, [4]Okide S, Njoku Obilor A.[6] and Dave [5]Ogbonna

[1]Department of Computer Science, Imo State University, Owerri
profoliverosuagtwu@gmail.com +2348037101792
[2] Department of Computer Science, Anambra State University, Uli, Anambra State
[3]Department of Computer Science, Federal Polytechnic, Nekede, Owerri
[4]Department of Computer Science, Nnamdi Azikiwe University, Awka
[5]Department of Network Engineering Technology, South Eastern College of Computer Engineering And Information Technology, Owerri
[6]Department of Computer Science, Federal University of Technology, Owerri

Abstract

Information Techology and associated tools have brought both blessing and curse to humanity. Inspite of awe-inspiring attacks of hackers and malware writers, the immense benefits of this technology has prevented many from withdrawing from its use. Just any one is affected by the services of Information Technology - Transportation Systems, Personal and corporate financial records and systems, Banking and financial institutions, Hospitals and the medical community, The public telephone network, Air Traffic Control, Power systems and other utilities, The government and the military. No body is left out. To prevent the collapse of the internet, the Internet Workforce, the industry have pooled resources together to provide some mitigation or palliative strategies, but these efforts have been inadequate to prevent continuing massive attacks by hackers. The attacks are becoming daring and more complex. The most advisable mitigation approach is to take the proactive route for survival. This paper has provided a modest list of emerging attacks on corporate information systems, a catalogue of the motivators, intension of hackers and sketches out a model of proactive mitigation response model for individuals and corporations.

1.0 Introduction

When we look at few statistics on Cyber warfare, one would ponder if the ascendance of Information Technology application is a blessing or a curse. For example, in January, Riptech announced it had culled more than 128,000 attempted attacks on 300 Riptech customers over six months. And in March, Predictive Systems amassed more than 12 million malicious-looking events from 54 sensors around the world in just three months equating to 90 attempted attacks per second). The Riptech study found 30 percent of all attacks came from computers in the U.S.; next was South Korea, at 9 percent. In fact, five of the top 10 sources of attacks were computers in Pacific Rim countries. In terms of intensity, i.e. attacks per Internet user, Israel far outdid any other nation [6]. According to [7] Chinese hackers already have unlawfully defaced a number of U.S. web sites, replacing existing content with pro-Chinese or anti-U.S. rhetoric. In addition,

an Internet worm named "Lion" is infecting computers and installing distributed denial of service (DDOS) tools on various systems. In 1999, FBI Computer Crime & Security Survey observed that out of 521 security practitioners in the United States, 30% reported system penetrations from outsiders, an increase for the third year in a row, 55% reported unauthorized access from insiders, also an increase for the third year in a row, Losses due to computer security breaches totaled (for the 163 respondents reporting a loss) $123,779,000 averaging a loss of [8]:

$759,380. There are more than 403 million unique known malware variants, and more than 55,000 known malicious web domains. Symantec software blocked 5.5 billion malicious web-based attacks in 2012 alone, 315 mobile device vulnerabilities were discovered in 2011. At least 232 million identities were maliciously exposed in 2011. The major US government defense agencies reported an average of 10 million cyber-attacks per day, per agency [10]. Recently (2008-2013) Verizon gave an overview of security breaches in Fig. 2 below

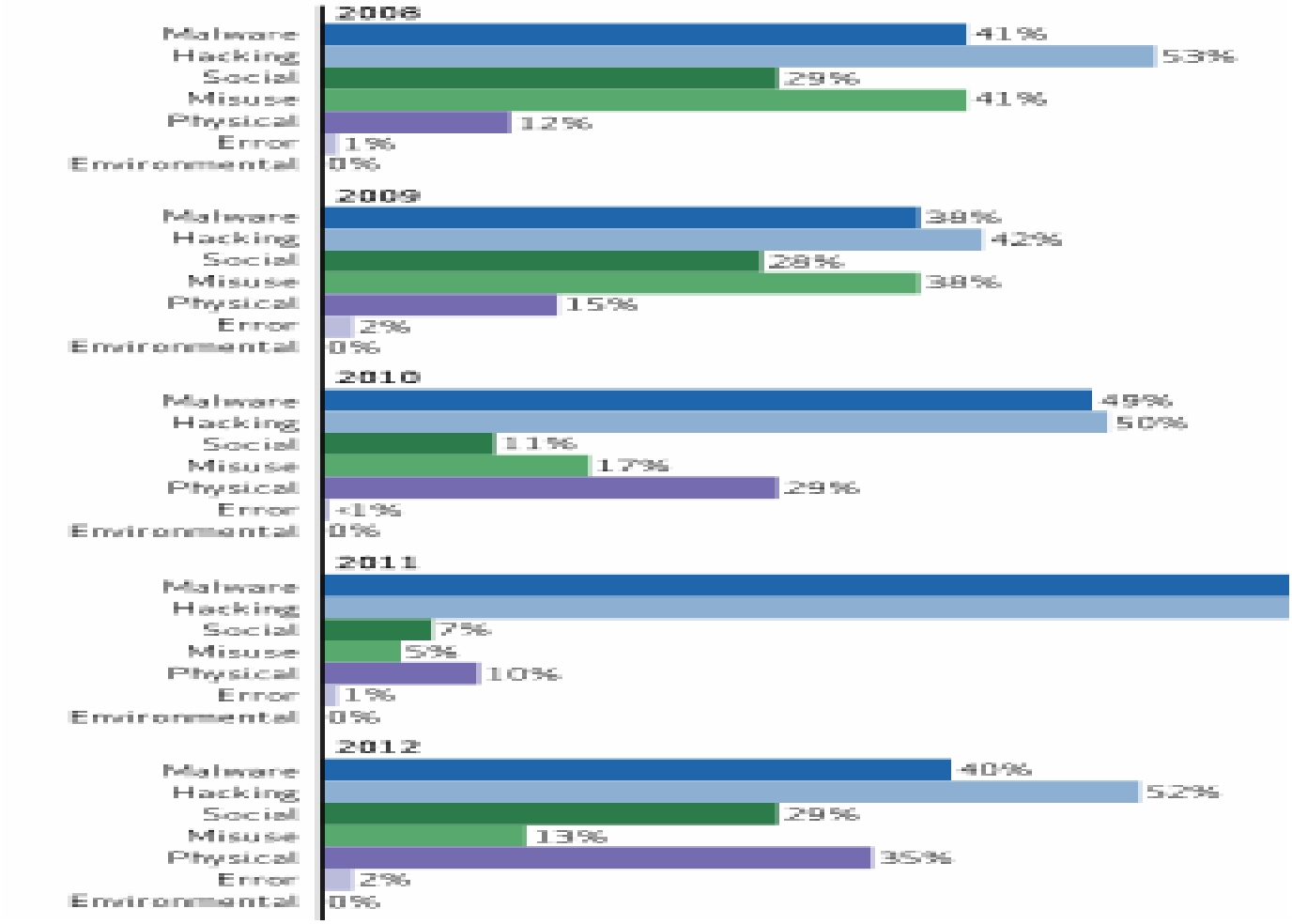


Fig. 1.8: 2013 Data Breach Report [source:(Verizon)]

Fig 1.8 observes a mixed growth from 2008 to 2013 in all the variables reported – Malware (47% in 2008 was down to 40% in 20012, hacking increased from 52% to 53% in 2012, an increase of only 1%, Social remained static from 29th in 2008 to 29% in 2012, Misuse was down from 41% in 2008 to 13% in 2012. This may be due to some proactive measures taken by management. Physical rose from 12% in 2008 to a whooping 35% in 2012! Error only marginally rose from 1% in 2008 to 2% in

2012. Environmental factors remain no threat as it earned no score in 2008 and 2012. According to ITU [9] Botnets', or as the media calls them, 'Zombie Armies' or 'Drone Armies', and their associated malware have grown over the years into a multimillion dollar criminal economy, which now constitute huge risk to government, critical infrastructure, industry, civil society and to the broader Internet community. That is what the current situation is! The threat is real!!

Corporate Information is the most valuable asset to all firms. If some trade secrets stored in the organizations data bases are compromised, the firm might be heading to a failure trajectory with its concomitant negative consequences for the national economy. It is therefore imperative that such information systems be protected from the massive attacks of hackers and malware writers. Security is about *regulating access to assets.* Thus, the goals of any corporate security policy are based on the CIA Triad [1]:

- Confidentiality
- Integrity
- Availability
- (authentication)
- (non-repudiation)

The three variables that constitute the Triad include ***confidentiality***, ***Integrity*** and ***Availability***. **Authentication** supports Confidentiality and Integrity while **non-repudiation** adds value to the concept of Integrity during business transactions

Confidentiality refers to the assurance that information is shared only among authorized persons or organizations. Breaches of confidentiality can occur when data is not handled in a manner appropriate to safeguard the confidentiality of the information concerned.

Integrity is the ***assurance*** that data cannot be created, changed, or deleted without proper authorization as such would compromise the confidence placed in such valuable asset.

Availability is the **a**ssurance that the systems responsible for delivering, storing and processing information are available 24/7 and accessible when needed, by those who need them and authorized to use such information. [2]

Webopedia [3] has defined ***authentication*** as the process of identifying an individual, usually based on a username, password, biometrics such as finger print or voice recognition. Thus, in computer security systems, *authentication* is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication ensures that the individual is **who he or she claims to be**, but says nothing about the access privileges of the individual.

Non-repudiation:

Web Dictionary [5] defines Non-repudiation as a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. But this specifically refers to online transaction. In digital communication, it specifically refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

The summary of the foregoing discussion is encapsulated in Fig. 1.1 below.

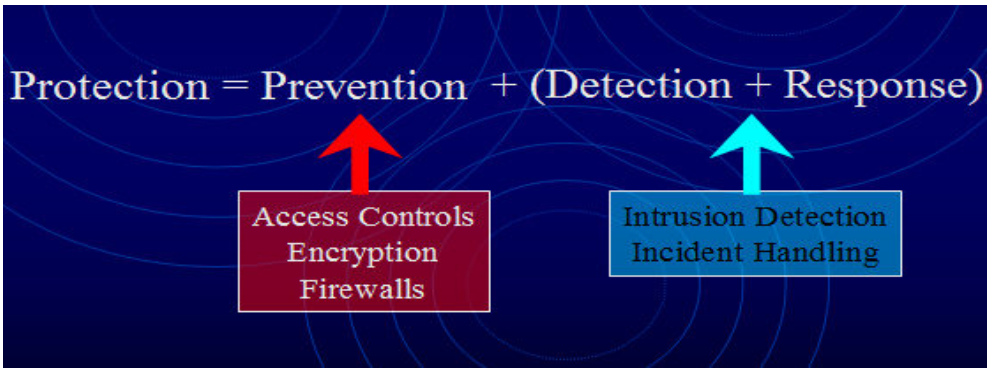


Fig. 1.2 Corporate Computer Security Operational Model [ ]

Fig. 1.2 is in essence saying that to protect Corporate Information systems require some proactive response model such as providing protection via Access Controls, Encryption and proper setting of Firewalls; Detection and Response which includes Intrusion Detection and Incident handling

Most security problems can be grouped into one of the following categories:

- Network and host misconfigurations
- Lack of qualified people in the field
- Operating system and application flaws
- Deficiencies in vendor quality assurance efforts
- Lack of qualified people in the field
- Lack of understanding of and concern for security

Organizations may approach attacks proactively or reactively. Most organizations only react to security threats, and, often times, those reactions come after the damage has already been done.

The key to a successful information security program resides in taking a *pro-active* stance towards security threats, and attempting to eliminate vulnerability points before they can be used against the firm. Other threats are created via weak security in TCP/IP, Eavesdropping, Theft of valuable information, Fraud, Authentication and Non-repudiation.

Cyber Warfare

The security challenges facing e-rganizations today is analogous to pure combat warefare**.** The description of the following battles confirms this assertion. Some of these treats include Identity spoofing, Denial of service, Loss of privacy, Loss of data integrity, Replay attacks, Viruses, Spyware, Trojans and other Malicious Software such as Botnets, Phishing, Spam, Cyber Stalking, Cyber Bullying and Online Predators etc. One of the worst vulnerabilities that can hit a corporate network is the virus/worm outbreak. Such attacks can tie up networks, cripple mail servers and disable many individual PCs [12].

Some definitions and grouping of illicit activities in the Cyberspace.

- *Hackers*: They enjoy intellectual challenges of overcoming software limitations and how to increase capabilities of systems.
- *Crackers*: These of hackers who illegally break into other people's secure systems and networks.
- *Cyber Terrorists*: This group of attackers threaten and attack other people's computers to further a social or political agenda

Hacker Motivation.

The following factors are part of the intrinsic motivators that let them do what they do:

- *The challenge* – we want to tell the world of our technical prowness.
- *Ego* – placing oneself on top of society

- *Espionage* – act as agent for others for financial gains.
- *Ideology* - a belief system such as secrets should done away with and let the world be transparent (Wiki Leaks).
- *Mischief* – to cause mayhem and disrupt social processes
- *Money (extortion or theft)* – to make money
- *Revenge* – to respond to previous maltreatment say by past employer.

Hacker Characteristics:

They are predominantly male folks. Most are aged from mid-teens to mid-twenties and they lack social skills. Most have fascination or obsession with computers and a good proportion of them are underachievers in order areas of human endeavour and see computing as a means of becoming important and powerful in society [4].

For ***Malware writers***, their motivations include the desire to see how far the virus can spread. The second motivator is to cause damage and destruction to a targeted individual or organisation. Others include the desire to achieve a feeling of superiority/power and to leverage some form of personal gain. Finally, they intend to use their technical prowess to teach some lessons to the Internet communication and to conduct some experiments.

Attack Pattern and Threats

We would like to precede attack patterns with some important defintitions**:**

- ***Vulnerability***: A flaw or weakness in system security procedures, design, implementation, or internal controls that may result in a security breach or a violation of the system's security policy.
- ***Threat***: The potential for a specific vulnerability to be exercised either intentionally or accidentally
- ***Control***: measures taken to prevent, detect, minimize, or eliminate risk to protect the Integrity, Confidentiality, and Availability of information.
- ***Vulnerability Assessment***: The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system
- ***Vulnerability remediation*** is the process of fixing vulnerabilities. Remediation choices
- For every vulnerability there are three choices for remediation -Fix - eliminate vulnerability altogether, Accept - the cost of fixing outweighs the risk, Mitigate – do not outright fix but use additional layers of security to lessen the risk presented by the vulnerability
- You should arrange to plan to remedy all vulnerabilities found in the system. This plan must include whether to fix, mitigate or accept vulnerabilities or Whether to use automatic or manual remediation Strategy to mitigate any remaining vulnerabilities and try to justify why a vulnerability should be accepted as it is without spending extra financial resource on the threat..

Malware Writers

These are a group of attackers responsible for the creation of malicious software that infects and destroy information systems**.** Malware is Malicious Software - deliberately created and specifically designed to damage, disrupt or destroy network services, computer data and software. There are several types. It includes viruses that conceal themselves, infect computer systems, replicate themselves and deliver a *payload*. ***Worms*** are Programs that are capable of independently propagating throughout a computer network. They replicate fast and consume large amounts of the host computers memory. ***Trojan Horses*** **are computer programs** that contain hidden functionality that can harm the host computer and the data it contains. Trojan Horses are not automatic explicators - computer users inadvertently set them off and attacks commence.

Software Bombs are Time Bombs usually triggered by a specific time/date. ***Logic***

Bombs are triggered by a specific event. Both are introduced some time before and will damage the host system.

Samurai

These are hackers hired to legally enter secure computer/networkenvironments for nefarious objectives or to check the vulnerability of the network to various forms of attack**.**

Phreakers

This group of attackers focus on defeating telephone systems and associated communication technologies.

Phishing

This group specialize in sending out 'scam' e-mails with the criminal intent of deceit and extort. Thus, *Phishing* is a technique used by strangers to ***fish*** for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number. These messages often contain company/bank logos that look legitimate and use flowery or legalistic language about improving security by confirming your identity details. This is becoming very rampant. You see in your email box your banker's logo and form format requesting you to fill your secret details. If you do, your email will automatically be compromised and the hacker will seize your password and change it to his and take full control of all communications sent to you. The programs are java applets which automatically installs themselves once you open the mail!

Spam

This is the main source of criminality particularly in Nigeria. It involves sending of unsolicited and/or undesired bulk e-mail messages, often 'selling' a product targeting of instant messaging services. The promise of disproportionate benefit to themselves and tries to extort some money deceitfully**.**

Zombie Computers

These are computers dedicated for fraud or systems used by 419 crooks to do illegal activities.

Defacing Websites

Hackers can leave their presence on other people's websites by defacing form example a Catholic Church website with nude women. Many sites have fallen foul of this activity and they include FBI, CIA, NASA, British Labour and Conservative Parties and New York Times as well as Conservative Party Website Hacked and Defaced 1997.

Denial-of-service (DoS)

DoS involves or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended legitimate users through some of the attacking techniques already discussed.

SQL Injection Attacks

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution.

Mitigation and Counter Measures

There are two basic approaches used to deal with security vulnerabilities: These are ***proactive*** and ***reactive***. Proactive approaches include all measures that are taken with the goal of preventing host-based or network-based attacks from successfully compromising systems. Reactive approaches are those procedures that organizations use once they discover that some of their systems have been compromised by an intruder/hacker or attack program. We shall now discuss these two approaches and mitigation strategies adopted. Both are not opposing forces. There is need to find a balance between how many resources can be devoted to proactive measures designed to deter network attacks, and how much to devote to reacting to intrusions [12]

Proactive measures:

These may include physical security of building, screening of personnel, legal framework to deter criminals and training of employees. Encryption is the strongest link we have for securing data. Everything else is worse: software, networks, people.

Setting up Security Monitoring Plan

The purpose of this plan is to identify suspected access violations and attempted system intrusions. A sample plan for example is:

- ***Daily review of remote access log-ins*** to identify failed access attempts.
- ***Review of system access logs*** for access to systems during non-work hours.
- ***Review of traffic*** on external gateways
- Review of access to application system utilities and privileged user activities
- ***Review of access*** to sensitive files or data Monitoring licenses registered versus licenses used
- Inventorying of PC software
- Developing and distributing approved software lists
- Developing software usage policies
- **A physical security plan** should check the use of Cipher or key pad locks, Fencing, Guards, Monitoring devices, Maintaining authorized personnel access lists, Limiting access to only essential operations personnel, Maintaining sign-in logs and Badges
- **An environmental security plan** would include Backup power (UPS) Air conditioning, Fire suppression devices (fire extinguishers, halon, other), Fire detection devices (sensors), Heat detection devices, Business continuity plans, Alternate processing facilities and Disaster recovery plans, System and data backups.

Backup and Recovery

Backups are critical and must be performed so that system, program, or information loss or damage can be efficiently restored. Backups should be stored away from the processing facilities. Tape management techniques need be reviewed often.

Risk Assessment

Deployment of IT for corporate information services is a risk. An Information Systems Manager ought to ponder what could happen (threat event)? If it does happen, how bad could it be (threat impact)? How often could it happen (threat frequency, annualized)? And how certain are the answers to the first three questions (recognition of uncertainty)?

Risk Management

This involves questions on what can be done (risk mitigation), how much will it cost (annualized) and is it cost effective (cost/benefit analysis)?

Business Continuity Planning (BCP)

Integrate the following phases into your BCP policies;

- Awareness and discovery
- Risk assessment
- Mitigation
- Preparation
- Testing
- Response and recovery

Risk and Impact Analysis

The firm should attem to identify her assets, determine vulnerabilities, estimate the likelihood of exploitation, compute expected annual cost, survey applicable controls and their costs and project annual savings attributable to control**.** An estimate of the probable cost may include Estimate of Expected Loss such as Legal obligations for preserving confidentiality/integrity, Business agreements on the expected service, Cost due to public disclosure, Benefit to competitor due to compromise of data, Loss of future business, credibility, Computational cost and outsourcing possibility, Value to other from the data and Cost of data recovery or reconstruction

Impact Analysis of possible attack would include the identification of what the enterprise has at risk, Which business processes are most critical, Prioritization of risk management and recovery investments, Identifying the enterprise's vulnerability to risks so that they can be mitigated in the project design phase.

Key Management (KM)

KM is a Set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. It involves the initialization of system users within a domain, generation, distribution, and installation of keying material, controlling the use of keying material, update, revocation and destruction of keying material, storage, backup/recovery, and archival of keying material**.**

Configuration of Firewalls is critically important if information systems has to be able to contain the attacks at first level.

Other measures include:

- Update the software on your computer weekly (or more frequently)
- Install anti-virus and anti-spyware software and keep it up-to-date
- Use accounts and strong passwords
- Encrypt sensitive information
- Do not install unknown software from unknown sites
- Do not share your accounts/passwords
- Use password protected screen savers
- Deploy Biometric Authentication Systems such as Finger print, iris of the eyes, voice recognition.
- Deploy Intrusion Detection and Prevention System and effective firewall on your servers
- Do not use the same password for all accounts
- Change passwords frequently
- Use more difficult passwords on more sensitive accounts
- Use a password safe (but do not lose the master password
- Do not open unknown emails and attachments
- Visit only reputable web sites http://safeweb.norton.com/
- Do not reply to SPAM or Phishing emails
- Only login to servers for the duration needed - disconnect when done
- Do not let others use your computer irresponsibly
- Use a Credit card for online shopping
- Do not Give out your personal information in response to an *unsolicited* email, phone call, or voice mail. If you are in doubt If in doubt, call the company using another legitimate phone number (not the one provided in the email or phone call).
- New scams use social networking sites to get your background personal information
- Be cautious when using open wireless networks. Others using the network maybe be "sniffing" the network. Security Expert Claims Thieves Can Detect Wi-Fi In Sleeping Computers.
- If you *must* use a public computer, change the password on the account accessed using a secure computer ASAP

For individual Laptops, Implement passwords on the device, Backup your data frequently and test backups. Store backups away from the laptop. Encrypt sensitive information. Watch your laptop at all times. Keep your laptop in your possession at all times and do not leave it out in your hotel room. You can also lock up your laptop with some software. Do not leave your laptops in the car, it could be stolen. Some people have left their Laptops in their cars and came back to see their car windows broken and their laptops taken away.

Reactive Measures

These are measures taken after an attack has succeeded. It includes reporting to the cyber crime committee and EFCC for

tracking the culprits and their eventual prosecution and installation of *adhoc* measures to prevent further attacks. However, the damage has been done! Normally when the worse happens, management implements temporary countermeasures, especially when a rampaging worm or virus makes it impossible to wait for thorough testing and careful application of patches. Often, this strategy means following a defined incident-response plan and shutting down ports on firewalls and routers or blocking IP addresses. The ability to put together an incident-response team, notify all necessary parties (internally and externally), and follow clear guidelines for escalation of issues is integral to successful implementation of these countermeasures [11].

Summary and Conclusion

Corporate information Systems attacks are increasing daily with exponential complexity. This threat requires a strategically planned action by firms to put attacks at bay and ensure the CIA tenet of Confidentiality, Integrity and availability. A consolidated Information security unit need be set up in every organization to detect and prevent the growing trend of Dinial of Service attacks, phishing, and malware attacks. This unit should be equipped with the right tools. Deployment of mitigation strategy must come after critical risk analysis to avoid economic waste. Paying good attention to security and associated risks is bound to secure the most important asset of organizations.

.

References

[1] http://en.wikipedia.org/wiki/Information_security

[2] Ndigwe Chinwe, Osuagwu O.E. et. Al. (2013) ***Understanding Integrity in Networked Data Base Applications,*** **MicroWave International Journal of Science & Technology**, Vol.5 No. 1 December 2013

[3] http://www.webopedia.com/TERM/A/authentication.html

[4] Cybercrime by Steven Furnell (2002) p 47

[5] http://en.wikipedia.org/wiki/Non-repudiation

[6] *Missed Opportunity* By Scott Berinato, www.cio.com, Apr 2002

[7] ***Collateral Damage May Soon Have A New Definition. "China Warns Of Hack Attack" Washington TimesApril 23, 2001, Front Page***

[8] **Verizon 2013 Data Breach Investigation Report**

[9] ITU Botnet Mitigation Toolkit 2008

[10] DefenseNews 2012

[11] **Verisign Whitepaper (2005)** ***Managing Application Security in Business Processe*** **, USA**

[12] http://www.crime-research.org/library/Richard.html

Deploying Electronic Health Record (HER) and Information Technology for Resolving Health Disparity Challlenges

[1]Babatunde B. Olofin, [2]Oluchi A. Olofin, [3]Nkechi O. Ohadoma & [4]Comfort Nwamaka Agu

[1]Department of Computer Science, Federal Polytechnic Nekede, PMB 1036, Owerri, Nigeria
[2,3]Department of Dental Therapy, Federal School of Dental Technology & Therapy PMB 01473, Enugu, Nigeria
[4]Department of Human Kinetics and Health Education, Enugu State College of Education (Technical) PMB 01793, Enugu, Nigeria
[1]Cell: +2348033215972; Email: bbolofin@gmail.com. Cell: +2348034711552; Email: oluchiolofin@gmail.com
[3]Cell: +2348035902119; Email: angelohadoma@yahoo.com. *[4]Cell: +2347065241311; Email: comfortagu@gmail.com*

Abstract

This paper examines the importance and function of HIT in the handling of the health disparities among the racial and minority ethnic population. From researches and investigation on the utilization of health care based technologies, there were discoveries that certain kind of population, in the minority, was affected. Recent and evolving use of Information Technology in the healthcare sector among the population that is in the minority and ethnicity in critically observed, stressing the areas that utilize IT in these population different from non-minority group and highlighting the need for newer form of social means of communication in the health education and delivery sector. In this paper, the author highlights the capabilities of resolving health disparities challenges using the electronic health record (EHR) and Information Technology and the subsequent impact of health information technology in the health care industry. Furthermore, the article also identifies the notable challenges in the implementation of the EHR among the minority population, and vividly explains the possibilities of Health Information Technology (HIT) in the handling of the disparities in health.

Keywords: Health, Health Care, Health Disparities, Electronic Health Record (EHR), Health Information Technology (HIT), racial, minority, ethnicity

---

1.0 Introduction

The notable monumental developments in the Information Technology (IT) are evidenced in the transformation of the society use line today. The health care sector has introduced changes also as a result of Information Technology, especially in the areas of the public health biomedical research, administration and finance [2]. In view of these technological advancements, said that IT must play a prominent role in the re-design of the Information System in the health care for the enhancement of the quality of service to the patients. Moreover, the stakeholders in the health care are interested in the potentials of IT in solving the health disparities being experienced among minority populations [1] [9] [14]. In the evaluations of the popularities of deploying IT into the disparities in the health care system, the hindrances and e- health solution to be better understood. Moreover, since the health is gradually being implemented in different settings, there is the need to identify the challenges and possibilities in these settings. These identified challenges and possibilities would enable an approach that is evidenced. Based on designing, the development, and in deploying relevant tools and program applications, there would also be the facilitation of various approaches to the

development of the IT in the healthcare and enabling reasonable tracking and assessment of the cost, the processes and the outcomes.

2.0 Fundamentals of e-health records (EHR) and Health Information Technology (HIT)

2.1 Concept of Electronic Health Record (EHR)

Electronic Health Record is an emerging concept that can be described a standard way of gathering of all information about a patient or group of people electronically [11]. It can also be regarded as an electronic copy of information that can be distributed to all health care organization after necessary authentication. This sharing of information can be achieving by means of return based information systems interconnected by hardware infrastructures. The data transmitted may include statistical data, status of immunization, results of laboratory tests, and history of medical status and other relevant information about a patient. There should be the usage of the acronyms EHR, EMR and EPR interchangeably. EMR is an acronym for electronic medical record, which is referred to as the record of patients in the hospitals or any other clinically based environment, that could be a source of data for the HER [12] [15]. EHR is for an institution or a regularly body which may include hospitals ethnics, an integrated information system network to allow access to medical records of patients.

2.2 Capabilities EHR in Resolving Health disparities

There are much notable potential that patients and healthcare professionals can adopt in utilizing technology to manage their health and other healthcare services. Some health regulatory bodies such as centers medicine and medical services emphasizing the need for health care services to go beyond face to face contacts, but it should adopt the use of information technology related tools to increase the access of patients to information and treatments especially in the managing of illnesses that are chronic in nature [2] [19] [20]. Conventionally, the focus had been on the role of personal patients would be allowed access to their health information. The main difference between the EHR and the PHR is that patients do not have the accessibility or capability to control the EHR or EMR (Electronic Medical Record) [20].

In a survey conducted by the California healthcare foundation, 7% of respondent used PHR [24], which implied the limitations of the adoption of the PHR usage was 11%, while was higher in the West and 15% in California. Majority of the users (64%) responded thus its usage helped them to ascertain the accuracy of their health information and approximately 50% said it helped in sending mail to their health providers and for online renewal of their prescriptions [24]. Moreover, over 50% of the users of PHR said it helped to possess the knowledge of their health status and their doctors care for them. PHR users were younger, very literate and highly paid individuals, but the less educated whose income were lower and with chronic ailments derived their values with continuous consultation with healthcare professionals in the cause management of their health [24].

In another study of enrollees of Kaiser Permanent, the enrollees observed racism and ethnic disparities among those registered for the PHR. The data distributes those registered is as follows: African Americans (30.1%); whites (41.7%). Normally, those that have access to internet and of higher educational attainment would likely be higher in number. Nevertheless, the disparities in education, internet access and income were not accountable by race when observed in the disparities for the PAR registration [20].

The adoption rule of the utilization for the tools of health IT by which patients and healthcare provides may not provide the accurate data required. Despite this fact, there are some evidences that some of these patients and health provides are accessing health information systems developed by other organs whose core competence is not the health care. According to [17], about 160

million of American citizens have utilized health-based tools online. In view of the evidence, an average American obtain information from online resources in the diagnosing and treatment of various ailments, implying that the internet-based resource is the most accessible health information resource [3] [17].

The collection of the various tools used for this purpose is referred to as the consumer health informatics the (CHI) [4] [6] [5] [8] [7] [13] [10]. Despite the fact that these available tools are not distinguished at the moment, 33.3% of the users confirmed positively to the value of information accessed through this resource, and reliable facts abound that the tools have helped in the curing of some ailments in the patients [10].

There is no evidence yet on the assessment on the use of CHI among on the patient's minority (ethnic and racial) nationally. Nevertheless, there is some level of disparity in the digital usage of the CHI tools. Within the period 2000 to 2010, the number of use of the internet among the blacks and Latinos is almost twice the original value, from 11% to 21%. Within the same period, there was less of African American that access the internet. In the same way, the African Americans are behind the whites in the use of the broadband links at home and also less in number in the acquisition of desktop PCs (African American – 51%, whites- 65%) [22]. There is a measure of identity in the use of broad band based internet among the Latinos (US-born) and the whites, while the Latinos who are foreign- born do not have the same usage of the facility with their US-born counterparts. (US-born – 81%; Foreign-born -51%) [16].

Lastly, the emergency of the social media can be seen as a powerful resource in the health care sector. With the development of Web 2.0 in 2004, there are positive features that help in the finality of both the consumer and the application [18]. With web 1.0, there was a one way of communication of resources on the internet web 2.0 has the capability of permitting the user to include the content on the WEB, thereby enhancing sharing capability and collaboration [18]. Therefore, social networking is used in the description of the application program and tools in Web 2.0.

Potentials abound in the usage of the social media in solving the disparities in the health care when it is properly examined by race. Ministry of the Americans are higher users of the mobile devices in the accessing of internet a research study conducted by Pow research center, "Nearly two-thirds of African-Americans (64 percent) and Latinos (63 percent) are wireless internet users, and minority Americans are significantly more likely to own a cell phone than their white counterparts (87 percent of blacks and Hispanics own a cell phone, compared with 80 percent of whites). Additionally, black and Latino cell phone owners take advantage of a much wider array of their phones' data functions compared to white cell phone owners" [23]. The health care sector has witnessed the entrance of the social media in different aspects. There is the need to understand that the demands of consumers in the health sector by entrepreneurs can lead to aggressive business creativity [21]. Online-based patient sites or groups are evolving very rapidly in the social networking. There are many hospitals and medical center of academic institutions that are utilizing social media with over 300 channels of you tube and twitter ales which can be viewed online. According to [21], there is the irrigation of notable, hospitals from the use of experiments to specific utilization of social media in the recruitment of patients.

2.3 Health Information Technology (HIT) & Its Impacts

HIT is the interchange of information on health in an electronically-based environment [25]. The extensive usage of HIT in the health sector would enhance the class of care, prevention of medically-based errors, and reduction of costs, improve efficiency in administration, reduction of paper-based work, and enlarge the access of the people to healthcare that is affordable. There is also the need to ensure the privacy and protection of all the electronic data since the transmission

of this information is carried out electronically.

The use of HIT in the management of an individual's health information is a pertinent aspect of the dynamicity in the healthcare system. With HIT, the physician could manage the health of the patient by improved means of communication between the two of them. The uses of computers with other peripherals make it easier for the doctors, the patients and the providers of health in the storage, sharing, and accessing of individual's health information. Therefore, the use of computers in this manner can be regarded as HIT.

The benefits of HIT include: reduction of paperwork by the elimination of handwritten of data on patients; reduction of unnecessary medical-based errors because information can now be transmitted electronically; reduction of costs incurred on healthcare through the decrease of repeated laboratory tests being requested from different doctors and the elimination of space and time in filing of the physical medical records; and improvement of quality healthcare and the assurance of the accuracy of all medical information being accessed by the healthcare providers. Despite the fact that HIT has numerable uses, there are 3 types of HIT that may be affected as the development continues. They are personal health records, electronic health records, and electronic prescription.

3.0 Challenges to Implementing EHR among the Minority

3.1 Notable hindrances to e-health implementation

It is an established fact that there are disparities while adopting and utilizing the varieties in health information technology. For better understanding of the disparities, the possible barriers or challenges to the adoption and utilization of the HIT need to be carefully considered from different viewpoints: 1) the perspective of the healthcare system and the solution developers; 2) the patients, household and the health-carers; 3) the effect of technology; and 4) the environment where there is the usage of technology and the delivery and reception of care. In view of these, any challenge is any of these areas could affect the adoption of the health IT, its utilization and finally the outcome. Furthermore, if the challenge is of a natural phenomenon, for example, a particular group of people may benefit more than the other technological development.

The way of interacting of electronic gadgets by human beings in an environment that is challenging is area of human based factor engineering that need to be noted. The relationship of these interactions with people, the jobs to be done, and the environment with the technologies utilized for this purpose which are totally different for the minority patient. In other to cut health care costs, there is the deployment of many electronic gadgets into homes today, implying the increase of human-based environmental issues.

There are notable barriers that would make the physicians not to adopt the e-health implementation. They include: negative attitudes of the physicians towards technology and the information system to be deployed; the negative effect of HIT on the workflow in the clinic and lack of competent technical staff to helping the office staff and doctors; lack of communication between the electronic health record and the HIT systems; and lack of absolute discussion whereby the providers can share their ideas, thoughts, information by writing or by speech, or through their professional medium, with the use of the social media.

Among the underserved population, there are notable barriers to the adoption of the e-health implementation. These include: the need to understand the positive effect of HIT for the patients and clinicians; the perception that the implementation could create additional work for the patients thereby making it cumbersome to accommodate this new idea of HIT; lack of confidence in the electronic gadgets to be deployed, technical challenges, mix-up in the educational materials or contents, limitation in accessing IT-based devices, anxiety in the use of the technology. In case of minority patients, the

barrier is the additional responsibility of caring for the family. Other barriers include poor knowledge of computer usage and the irrelevance of culture, lack of privacy and confidence in those that would handle the information supplied.

3.2 E-health solutions for Health-care Disparities

HIT may impact the determinant of the disparities of healthcare service providers. The aim of the provision of health IT-based tools for the care of the patients is to make available the information in a simplified way that the patients would embrace the technology. When this is achieved, the patients would believe in the accuracy of their health information instead of the manual manner in which the medical records have been kept. Moreover, once the patient's information is found to be accurate in the electronic health record (EHR), there would be increase in usage of the information, and there would also be reliance on the data. When this is consistently done, the resultant effect of the promotion of this reliable information would be admired and disparities among healthcare providers would be minimized.

The EHR would provide the doctors with relevant information on various options available for treatments, with an aim of the provision of clinical support, thereby making the clinician to offer a classical treatment. This tool could also help in the provision of an effective decision-making support in the generation of feedbacks on the performance of the clinicians by generating reminders, standardized reports, or clinical assessments. The reminders and the standardized reports would provide feedbacks to the health-providers on the standard or classic of healthcare provided to such a patient. When specific indicators on disparities are included in the report, this kind of information could reduce any form of disparity by the exposition of unacceptable practices in the clinic that is not of the standard expected and this would help in noting the performance of such provider over patients serviced. When such information is made available to the providers, the identified areas of disparities would be handled by the providers, thereby attending to areas of improvement.

There is the possibility of the synergy between the HIT and the physician-patients connectivity. Tools to be used for the connectivity are email, electronic means of consultation (known as e-consultation), electronic prescription (known as e-prescription) and EHR systems in enabling the providers in connecting with their fellow professionals. With these tools, there would be the facilitation in reducing disparities in healthcare. Moreover, there would also be the provision of standby access to the needed expertise in facilitating improved diagnosis and curative decisions. Other tools that could reduce the healthcare disparities are telemedicine, remotely-controlled monitors and sensing devices, patient's email, and the use of Internet-based social media, in connecting healthcare providers and systems to the patients and health-cares. Furthermore, the use of these HIT tools would reduce disparities by providing care, educating them, or supporting the disparity people and assisting them to have access to care that is not available. If these tools are not evenly utilized across different population, disparity is evitable.

Ensuring the increase way of regular checking of the pertinent parameters in the clinic among the minority (racial and ethnicity) patients would enhance the connectivity between the providers and the patients, which could impact disparities in healthcare. Due to the poor self-management of some patients in failing in the monitoring of their health status, technology-based devices such as patient-sensor can be remotely-enabled to monitor and deliver results to a compatible device or to an electronic health record (EHR). There could be the facilitation of enhanced management of clinical and disease-control case, which would result in fewer cases of complication, and ultimately reducing disparities. The above-stated IT tools could help in the facilitation of stabilized relationships

between the providers and the patients by enabling the patients to have undistorted means of communication, access to care, or ensuring the provider relationship is maintained. Moreover, these tools would also help in the promotion of care for the patients, facilitation of a shared form of decision-making, and an enhanced patients' centrally-controlled form of care, which sum up to good quality of care.

Finally, the use of HIT tools offers a futuristic promise in the support of the behaviour of the patient's health. When the social assistance and means of interaction are enhanced, the usage of these tools would increase the engagement of the patients, especially among the population in the minority whose use of mobile devices as a means of communication and social media are higher than the population of the white.

4.0 Conclusion

There is a great potential and futuristic promise in HIT usage among the minority population (in racial and ethnicity). Yet, there is a dire need to overcome all the challenges (technically, practically, and humanly). To evaluate the success or the failure, there is need to conduct a research on the surveillance and observance of progress made nationally. Moreover, due to the different forms of technologies, user-types, and the environment for the deployment of such information system, it would be a great challenge to collate the accurate information on the adoption and the use of such systems. With the effective usage of the HIT by the providers, there is the possibility to monitor its utilization by the providers among other participating health providers. In addition, with the usage by the patients to access, manage, and use of their health information, there could be the need of developing a meaningfully patient-use form of criteria.

Sequel to these developments and usage of HIT, there could be the need for certification of all the hardware and software for standardization and consistency in its usage among vulnerable group of people. Once these challenges are handled, there could be the need to develop patient-provider oriented-based HIT tools and other devices. As at now, most of these tools are designed and developed not in the healthcare settings. Therefore, as regards the potentials of HIT in handling the disparities in the healthcare, is whether there would be the acceptance of the evolving of HIT opportunities so as to achieve the aim of a better system of healthcare and a society that is healthy.

References

[1] Calman, N., Kitson, K. & Hauser, D. (2007). Using Information Technology to Improve Health Quality and Safety in Community Health Centers. Progress in Community Health Partnerships, 1(1), 83–88.

[2] Committee on Quality of Health Care in America. (2001). Crossing the Quality Chasm. Washington, DC: National Academy Press.

[3] Estabrook, L., Witt, E., & Rainie, L. (2007). Information Searches That Solve Problems. Washington, DC: Pew Research Center.

[4] Eysenbach, G. (2000) Consumer Health Informatics. BMJ 320 (7251), 1713–16.

[5] Eysenbach, G., & Diepgen, T. L. (2001). The Role of E-health and Consumer Health Informatics for Evidence-Based Patient Choice in the 21st Century. Clinics in Dermatology 19 (1), 11–17.

[6] Eysenbach, G., & Jadad, A. R. (2001) Evidence-Based Patient Choice and Consumer Health Informatics in the Internet Age. Journal of Medical Internet Research 3 (2), E19.

[7] Eysenbach, G., Powell, J., Englesakis, M., Rizo, C., & Stern, A. (2004). Health Related Virtual Communities and Electronic Support Groups: Systematic Review of the Effects of Online Peer to Peer Interactions. BMJ, 328 (7449), 1166.

[8] Eysenbach, G., Powell, J., Kuss, O., & Sa, E. R. (2002). Empirical Studies Assessing the Quality of Health Information for Consumers on the World Wide Web: A Systematic Review. JAMA 287 (20), 2691–2700.

[9] Gibbons, M. C. (2005). A Historical Overview of Health Disparities and the Potential of eHealth Solutions. Journal of Medical Internet Research, 7(5).

[10] Gibbons, M. C., Wilson, R. F., Samal, L., Lehman, C. U., Dickersin, K., Lehmann, H. P, et al. (2009). Impact of Consumer Health Informatics Applications. Evidence Reports/Technology Assessments, no. 188, 1–546.

[11] Gunter, T. D., & Terry, N. P. (2005). The emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. The Journal of Medical Internet Research, 7(1).

[12] Habib, J. L. (2011). EHRs, meaningful use, and a model EMR. Drug Benefit Trends, 22(4), 99-101.

[13] Keselman, A., Logan, R., Smith, C. A., Leroy, G., &. Zeng-Treitler, Q. (2008). Developing Informatics Tools and Strategies for Consumer-Centered Health Communication. Journal of the American Medical Informatics Association, 15(4), 473–83.

[14] Ketcham, J. D., Lutfey, K. E., Gerstenberger, E., Link, C. L., & McKinlay, J. B. (2009). Physician Clinical Information Technology and Health Care Disparities. Medical Care Research and Review, 66 (6), 658–81.

[15] Kierkegaard, P. (2011). Electronic Health Record: Writing Europe's health care. Computer Law & Security Review, 27 (5), 503-515.

[16] Livingston, G. (2010). The Latino Digital Divide: The Native Born versus the Foreign Born. Washington, DC: Pew Hispanic Center.

[17] Manhattan Research. (2010). Cybercitizen Health v9.0. New York: Manhattan Research, 2010.

[18] O'Reilly, T. (2005). What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. O'Reilly Media Inc. Retrieved August 26, 2012, from http://oreilly.com/web2/archive/what-is-web-20.html

[19] Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of Electronic Personal Health Records. BMJ, 335(7615), 330–33.

[20] Roblin, D. W., Houston, T. K., Allison, J. J., Joski, P. J., & Becker. E. R. (2009). Disparities in Use of a Personal Health Record in a Managed Care Organization. Journal of the American Medical Informatics Association, 16 (5), 683–89.

[21] Sharp, J. (2010). Social Media in Health Care: Barriers and Future Trends. iHealthBeat/California Healthcare Foundation. Retrieved August 26, 2012, from http://www.ihealthbeat.org/perspectives/2010/social-media-in-health-care-barriers-and-future-trends.aspx

[22] Smith, A. (2010a). Home Broadband 2010. Washington, DC: Pew Research Center.

[23] Smith, A. (2010b). Mobile Access 2010. Washington, DC: Pew Research Center.

[24] Undem, T. (2010). National Health IT Consumer Survey. California Healthcare Foundation.

[25] U.S. Department of Health & Human Services. (n.d.). Health Information Technology. Retrieved August 26, 2012, from

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/index.html

Laserjet Printer Troubleshooting Expert System

Adesola, W. A.[1], Ele, Sylvester I.[2] and Umoh, E. E.[3]

[1]Department of Computer Science, Cross River University of Technology, Calabar, Cross River State. shobisi@hotmail.co.uk
[2]ICT Development Department, Governor's Office, Calabar, Cross River State. el_silver2@yahoo.com
[3]Department of Computer Science, Cross River University of Technology, Calabar, Cross River State. enoimah@yahoo.com

Abstract

*This paper model an expert system called **LAPTEX** for troubleshooting LaserJet printers' faults.Today, with the innumerable advances in information technologies, computerizing printer's fault troubleshooting and identifying faults is far becoming so vital. Also, printers' fault detection is a complicated process that requires a high level of expertise (formal or informal) and depending on the know-how of the technician, a printer could be abandoned for just a minor fault. Our objective is therefore, to develop an Expert System for troubleshooting a LaserJet printer's faults. The Expert Systemis comprises of a user interface, a rule-base, an inference engine, and aknowledge editor interface. The system is meant to computerize the maintenance, and repair process of LaserJet printers, and give a time-based assistance to those who are in need of instant help when the maintenance experts are not handy.The method of fact-finding called knowledge acquisition which is a knowledge-based approach to extract facts was adopted. The methodology follows the waterfall model of software development life cycle. Java programming language platform was used to implement this system while Net Bean was used to draw the user interface (UI) design.*

Keywords: Expert System, LaserJet Printer, Knowledge-Base.

1.1. Introduction

Expert System is a knowledge-based computer program comprising of expert domain about objects, events, situations and causes of actions, which emulates the process of human experts in the particular domain [1]. It is also defined as an intelligent computer program that uses knowledge and inference procedures to solve problems that are difficult enough to require significant expertise. In other words, expert system is a computer application that performs an assignment that would otherwise be performed by a human expert.

Expert systems are one of the branches of artificial intelligence research. Although ExpertSystems do not actually "reason", they are able to apply information assembled from human experts by a knowledge engineer to new problems. Their suggested solutions to these problems can help users determine the best course of action. Artificial Intelligence's scientific goal is to understand intelligence by building computer programs that exhibit intelligent behavior. It has to do with the concepts and methods of symbolic inference, or reasoning, by a computer, and how the knowledge used to make those inferences will be represented inside the machine.

Much current work in artificial intelligence focuses on computer programs that aid scientists with complex reasoning tasks. Recent works has indicated that one key to the creation of intelligent systems is the incorporation of large amounts of task-specific knowledge [2].

Several Expert Systems have been developed performing different task ranging

from interpretation, prediction, design, planning, model-based to diagnostic and troubleshooting systems.

This paper, LaserJet Printer Troubleshooting Expert System, presents issues in the design of an Expert Systemwhile it aimed to develop an Expert Intelligence System for troubleshooting LaserJet Printer.

1.2. **LaserJet Printer Mechanics**

From manufacturer to manufacturer, and model to model, the exact arrangement and combinations of components can vary in laser printers. However, the order of operations is always the same. The six phases of operation in a laser printer include Cleaning, Conditioning, Writing, Developing, Transferring and Fusing. When character data is received from the host computer, it is converted into a serial bit stream, which is applied to the scanning laser. In Hewlett-Packard printers, the main portion of the printing system is contained in the electro-photographic cartridge. This cartridge contains the toner supply, the corona wire, the drum assembly, and the developing roller [3].

1.3. **The Need for the NewSystem**

At this age of information, it is required that all communication devices should be up and running. Printers are essential output devices attached to PCs which need to be functional at all time. Its down time therefore will prove vulnerable, and worst still, if there is no technician to fix the problem immediately. As noted by Kaushik et al [4], most computer users are amateurs when it comes to the age of troubleshooting. According to Deepaand Packiavathy [5], Expert system is justified when human experts are unavailable or unable to do the job. This Expert System is expected to help those amateurs who are in need of guides to deal with their LaserJet printer problems. Specific objectives of this system are:

i. To assemble a knowledge-based system that is common to the troubleshooting and intenance of LaserJet printers of various models.

ii. To present this knowledge in a diagnostic format such that will enable even a non-printer specialist solve their printer problems, and give time-based assistance to those who are in need of instant help when the maintenance experts are not handy.

2.0. **Architecture of the LAPTEX Expert System**

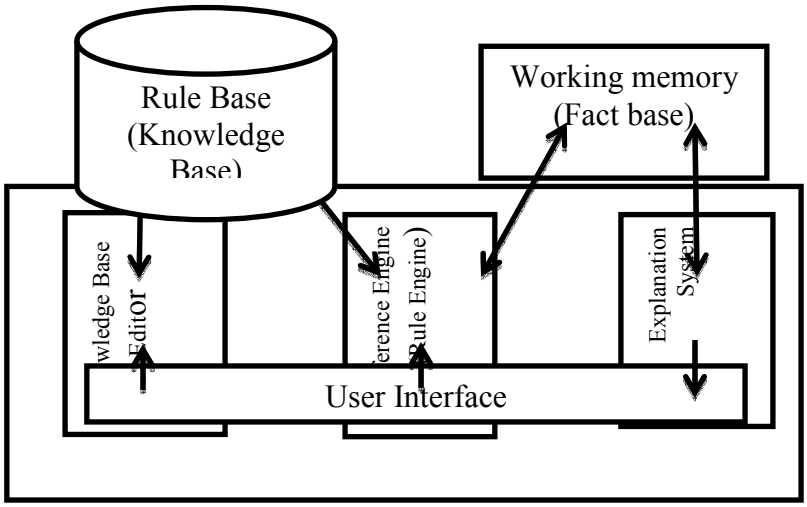


Figure 1: **Architecture the LAPTEX Expert System of the**

2.1. The User interface

The user interface is the means of communication between the user and the expert system problem solving process [6]. The user interface in this system will be able to accept instructions from user. Users will be asked several questions which they have to answer and will be displayed on the screen in responds to user's request.

2.2. The Knowledge Base

The knowledge base of expert systems contains both factual and heuristic knowledge. Factual knowledge is that knowledge of the task domain that is widely shared, typically found in textbooks or journals, and commonly agreed upon by those knowledgeable in the particular field.
In this study, knowledge acquisition was donethrough experts in printer repairs, service stations, documented printers faults etc.

2.3.TheInference Engine

This is the code at the core of the system which derives recommendations from the knowledge base and problem specific-data in the working memory [7]. It is the brain logical reasoning on rules and problem-solving strategies to draw answers and conclusions and infers new knowledge [8]. In the propose system, the authors adopted the goal driven or backward chaining inference technique using the IF-THEN rules to break our goal repetitively into smaller sub-goals for easy proving.

2.4. Different Types of Problem Modules in LaserJet Printer Faults

One of the biggest problems associated with any printer occurs when the wrong paper type, or paper type setting, is used. Because of the extreme complexity of the laser printer's paper handling system, paper jams are a common problem. This problem tends to increase in frequency as the printer's components wear from use. Expert System is able to detect those faults and also to suggest for possible rectification [9]. In the program for the application design, these faults were divided into different modules. The problems includes paper jammed, printer refusal to on, printer start up to offline mode, Image appeared watched out, printer produces missing beam errors, paper not feeding, and other miscellaneous faults

.

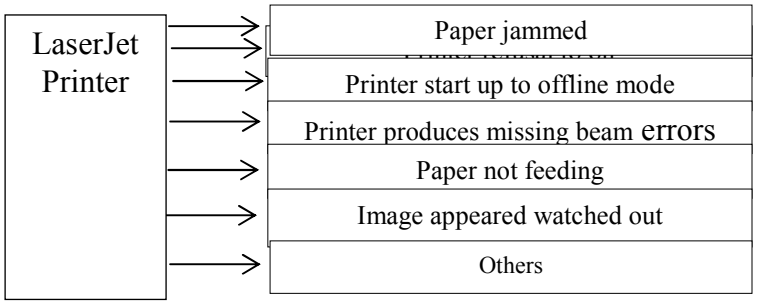


Figure 2: **Different Problem Modules of LaserJet Printer Faults**.

2.7. **Sample Data (LaserJet Printer Problem) for Knowledge-based Creation.**

Table 1:**sample Data (LaserJet Printer Problem) for Knowledge-based Creation.**

SYMPTOM	CAUSES	SOLUTION
Printer Does not start up	Power supply cord and outlet is bad Internal fuses are bad The motor and gear train is bad	Check all the normal power supply components. Check the internal fuses. Replace these components if they are gone bad.
Image appeared watched out	Power supply that serves the corona wire is bad. The Drum section of the printer is also faulty.	Replace high voltage section of the power supply. Allow printer to cool sufficiently and then replace the corona wire with a new one. Always avoid placing conductive instruments in the high voltage area.
Printer produces missing beam error.	The DC portion of the power supply has failed. The laser/scanning module is affected. Control board is affected.	Replace DC of the power supply.
Paper jammed	This is result from incorrectly setting the paper tray switches in a laser printer.	Troubleshoot the particular section of the printer where the jam is occurring-pickup, registration, fusing area, and output devices (collators and duplexers).

3.0. Methodology

The methodology adopted in the design of this system is presented in the figure 4 below. The methodology follows the waterfall model of software development life cycle and the 2.0 Specification of Unified Modelling Language (commonly known as UML 2) .Java programming language platforms was used to implement this system. The choice was as a result of features supported by the language. Java is a powerful programming language, it is portable, robust, multi-platform enabled, has rich library, simple, etc. [10].The key features are inheritance, polymorphism, reusability, knowledge representation, integration or extensibility. Java is an object-oriented language and it's used for opened distributed application [11]. Net Bean is used to draw the user interface (UI) design. It is efficient, effective and reduces time consuming to draw User Interface in writing desktop application with java.

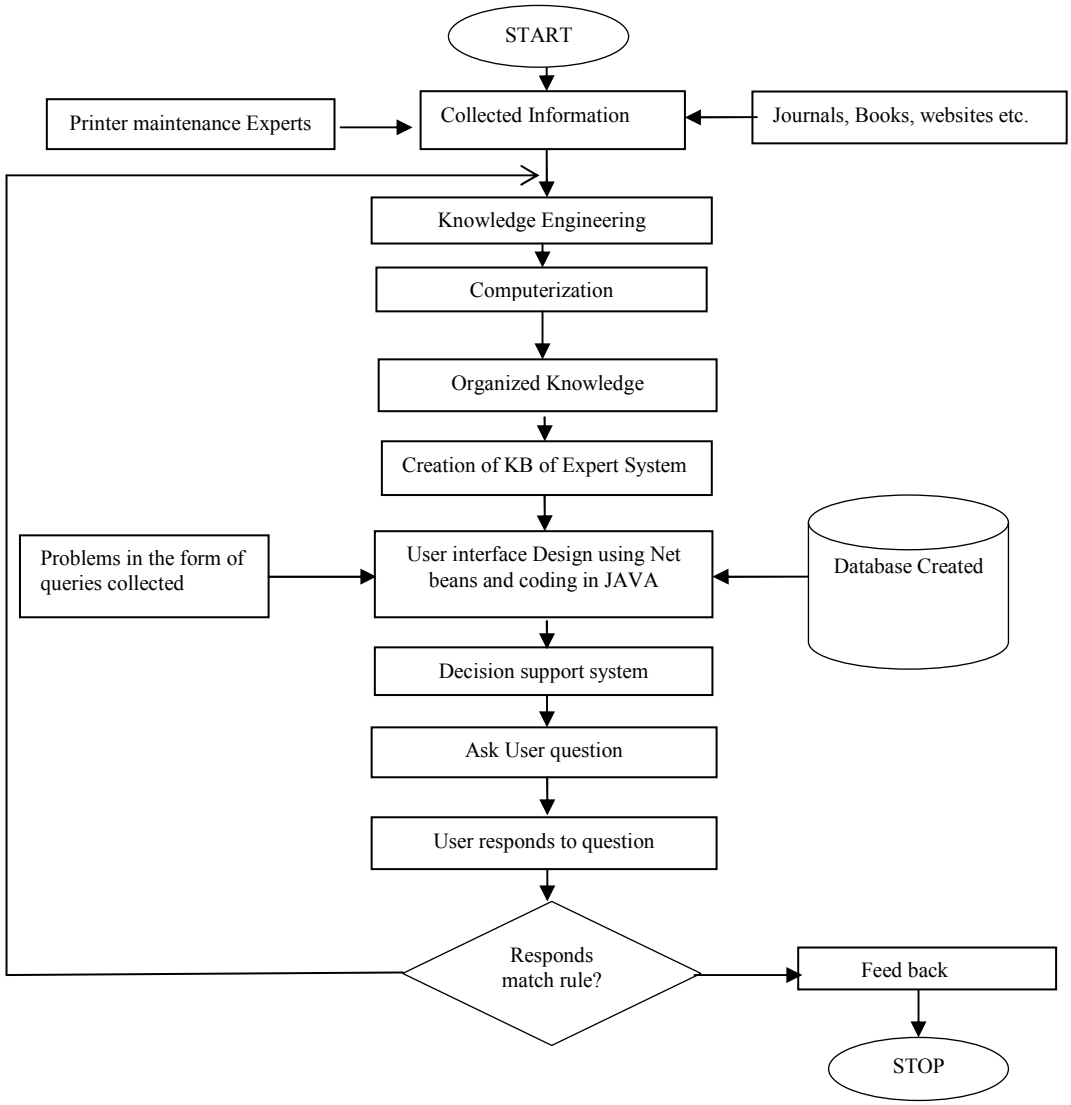


Figure 3: **Waterfall Model of the LAPTEX Expert**

3.1. **Algorithm of the LaserJet Printer Expert System**

Below is the algorithm used by the inference engine of the LaserJet printer (LAPTEX) troubleshooting Expert System.

Step 1: Get the facts and stored them in the working memory

Step 2: Check the condition part of the rule of the rule-base (at left hand side)

Step 3: If conditions matched, execute the right hand side (fire the rule).

ELSE

Repeat, if more facts are present

Step 4: Load the next facts and update the working memory with it.

Step 5: Goto step 2

Step 6: Use conflict resolution strategy to select more appropriate rule, and fire the rule if all conditions matched.

Step 7: Continue until all facts are treated

.

3.2. **Decision Tree for Knowledge base Creation**

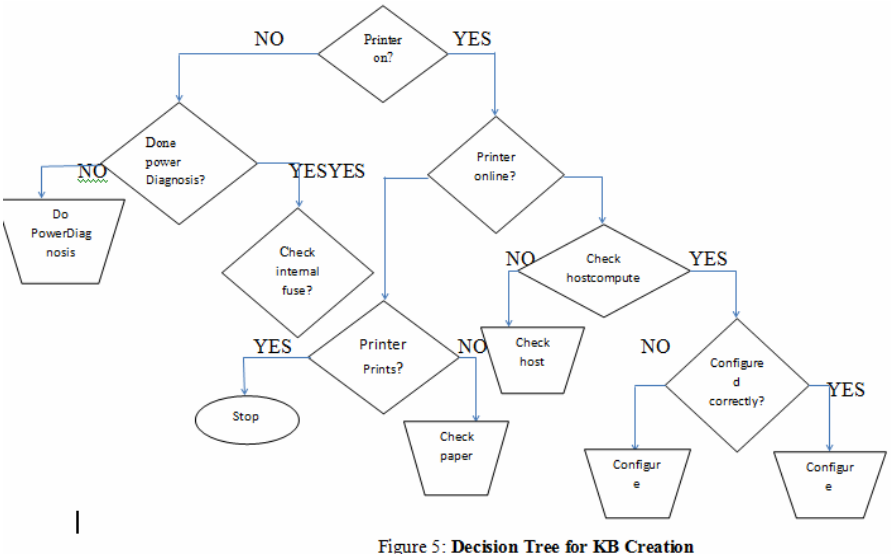


Figure 5: **Decision Tree for KB Creation**

3.3. **Sample Rules in the Rule-base**

I F *Printer is on*

AND *Printer is on to online mode*

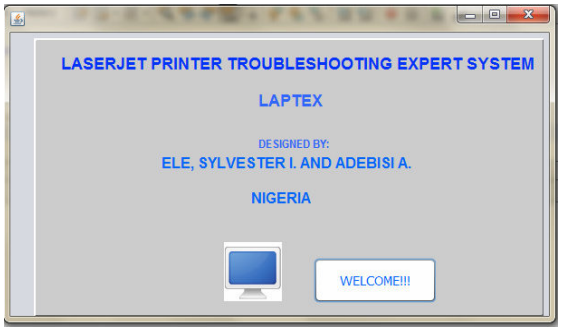
AND *Printer refuses to print*

AND *Red light lit on*

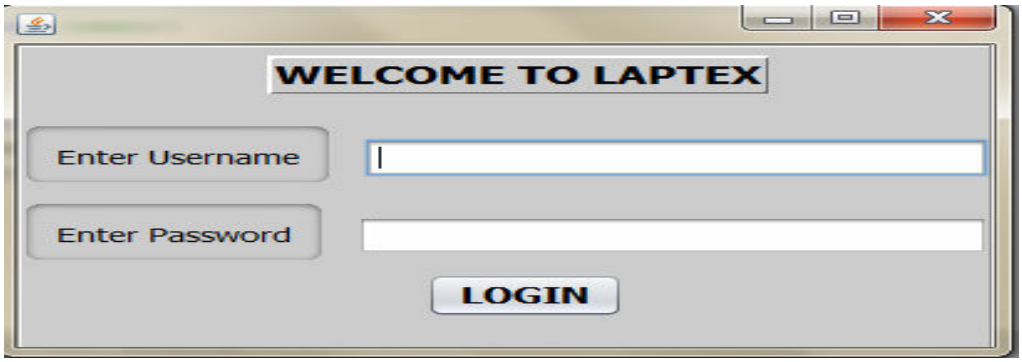
THEN There is Paper Jam or the right paper is not used. Use right size of paper.

4.0. **Implementation**

Java programming language platform was used to implement this system. The choice was as a result of features supported by the language. Net Bean is used to draw the user interface (UI) design. It is efficient, effective and reduces time consuming to draw UI in writing desktop application with java. Good and interactive user interface will encourage users to use the application [12]. A user friendly interface was designed in the system. When the user has launched the application after finishes all required installations. When the application has started, it display a welcome message printed in English language and prompts user to Click on "Welcome". When the user clicked the 'Welcome" button, system login form appears prompting the user to enter user name and user password. When user typed password correctly, it takes the user to the main screen (user interface screen), else, it respond with an error message.

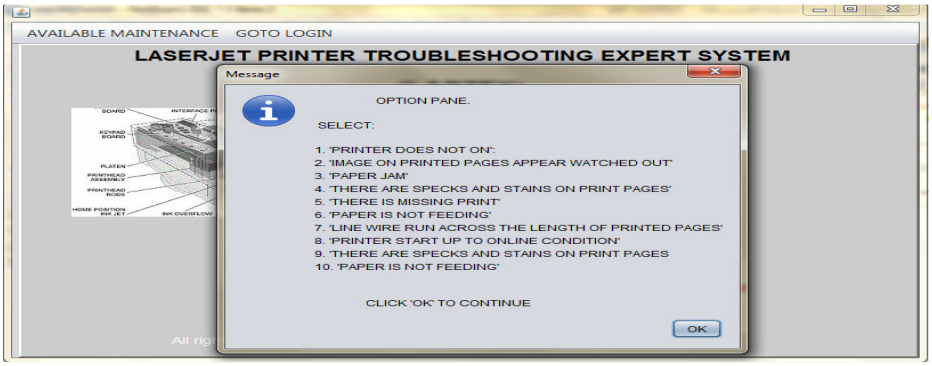


Display 1: **Welcome Message of the LAPTEX**

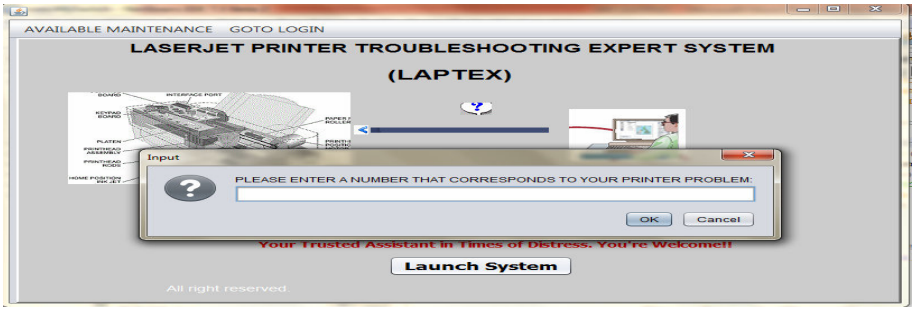


Display 2: System prompts Users to Login

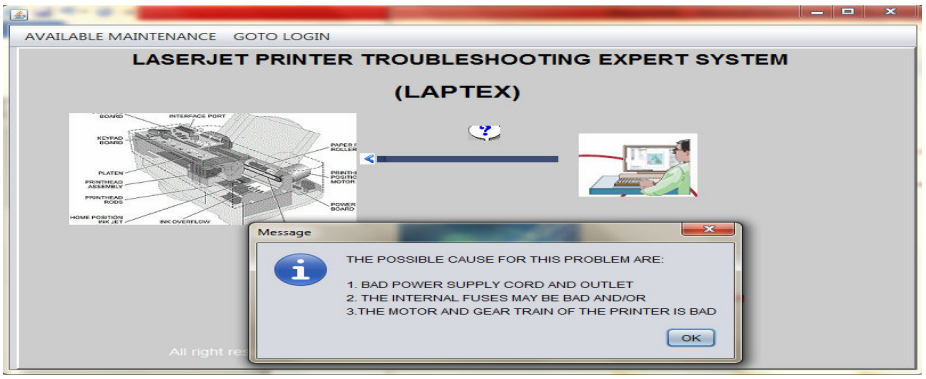
Display 3: **User Interface Main Screen**



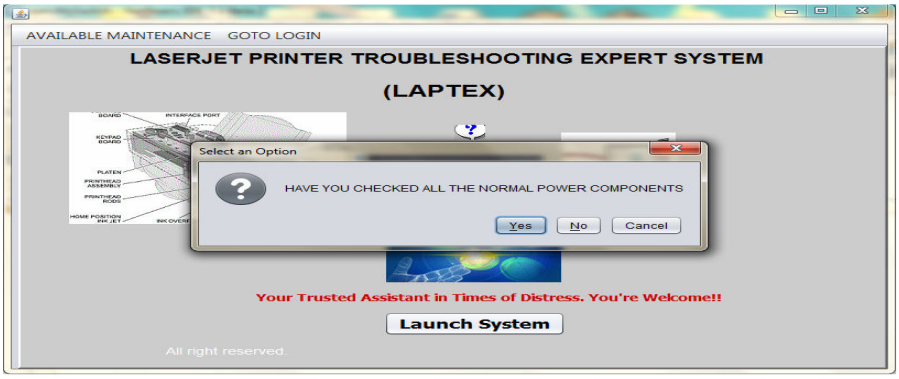
Display 5**: System Instructs User on how toInteracts with the Interface**



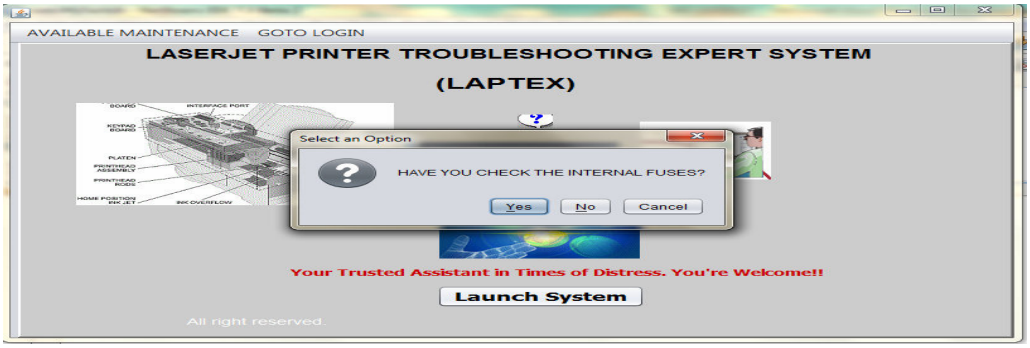
Display 6: **System Prompts User to Enter a Number that Corresponds to his Problem**



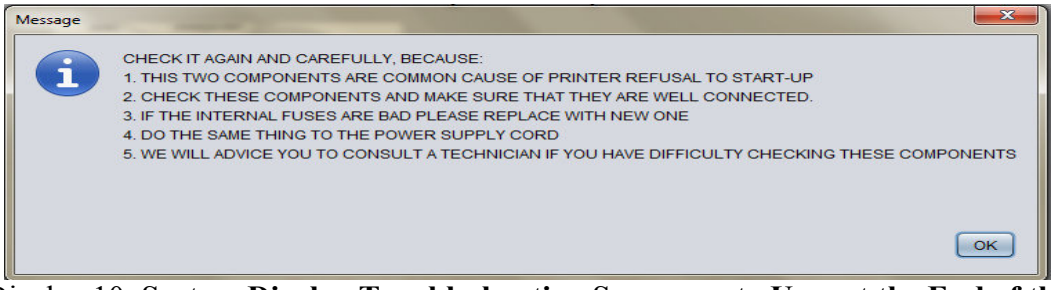
Display 7: **System Responds to User Request.**



Display 8: **System Starts a YES or NO Query with the User as Troubleshooting Begins**



Display 9: Query continues



Display 10: **System Display Troubleshooting Summary to User at the End of the Interactions.**

5,0 Conclusion

This paper presents Expert System to troubleshoot LaserJet printer's faults. The System, LAPTEX, was develop and tested. It diagnoses the problem, and gives advice to the user on how to locate the exact cause of the problem and to repair it.

References

[1] Sekari, G. G., Srinat, M. and Veluchamy, G. (2005). "Expert System – An Innovative Tool for Managing Indian Traditional Medical Knowledge", 9th World Congress on Health Information and Library, Salvador-Bahia, Brazil, September, 2005.

[2] Brook, C. (2002). "A+: Training Guide (4ed)", Que Certification, USA.

[3] Van Melle, W., Shortliffe, E. H. and Buchana, B. G. (1981). "EMYCIN: A Knowledge Engineer's Tools for Constructing Rule-based Expert System".

[4] Kaushik, A., Satvika and Barnela, M. (2012). "Printer Troubleshooting Expert System". In the Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, Issue 10..

[5] Deepa, S.T. and Packiavathy, S. G. (2012). "Expert System for Car Troubleshooting". In the Journal for Research in Science & Advanced Technologies vol.1 (1), Pp. 47, August 2012.

[6] Verma, Jindal & Aggarwal, J. (2010)."An Approach towards designing of Car Troubleshooting Expert System", In the International Journal of Computer Applications, vol. 1Issue 23.

[7] Chakaborty, R. C. (2010). "Expert System". AI Course Lecture. www.myreaders.info/html/artificial_intelligence.html

[8] Basil, Y. (2012). "Expert PC Troubleshooting with Fuzzy-Logic and Self-Learning Support".In the Journal of Artificial Intelligence and Application (IJAIA), vol. 3, No.2 March 2012.

[9] Sourav, M., Chatterjee, S. and Neogi, B. (2013). "Diagnosing and Troubleshooting of Computer Faults Based on Expert System and Artificial Intelligence, In the International Journal of Pure and Applied Mathematics, Vol. 8 Issues 5, 2013.

[10] Su Myat, M.S. and May P.P.Z. (2008).''Design and Implementation of Rule-based Expert System Fault Management", in The World Academy of science, Engineering and Technology, vol.48.

[11] Adams, D. et al, "Oracle Database Application Developer's Guide Fundamental, 10g Release 1(10.1)", 2003. Oracle Corporation

[12] Japheth, B. R. and Bubou, G. M. (2012). "Expert System Design for PC roubleshooting". In the Journal of Physical Sciences and Innovation, Vol. 4, Pp. 21, September 2012.

Deploying Java Platform to Design A Framework of Protective Shield for Anti– Reversing Engineering

[1]Okonta, Okechukwu Emmanuel, [2]Wemembu, Uchenna Raphael, [3]Ojugo, Adimabua Arnold), [4]Ajani, Dele

[1] Department of Computer Science Federal College of Education (Tech) Asaba.
[2] Department of Mathematics Federal College of Education (Tech) Asaba.
[3]partment of Math/Computer Sc Fed University Petroleum Resources Effurun
[4] Department of Computer Science Federal College of Education (Tech) Asaba

Abstract

Java is a platform independent language. Java programs can be executed on any machine, *irrespective of its hardware or the operating system, as long as a Java virtual machine for that platform is available. A Java compiler converts the source code into "byte-code" instead of native binary machine code. This byte-code contains a lot of information from and about the source code, which makes it easy to decompile, and hence, vulnerable to reverse engineering attacks. In addition to the obvious security implications, businesses and the wider software engineering community also risk widespread IP theft - proprietary algorithms, for example, that might be implemented in Java could be easily reverse-engineered and copied. This paper addresses the problem of reverse engineering attacks on software written in Java. It analyzes the present protective techniques used to protect software from such attacks, examines their limitations and provides a new tool that implements several anti-reversing techniques. This novel tool is code named KDefender and it drew its concept from ANTLR- ANother Tool for Language Recognition*.

Key words: JAVA, Anti-Reverse Engineering, byte-code, Re-Engineering, Obfuscators, KDefender

---

Introduction

The process of extracting knowledge or design blueprints from anything man-made is known as reverse engineering [19]. So in real terms, reverse engineering may be understood as a systematic methodology for analyzing the design of an existing device or system, either as a way to study the design or as a means for re-design. "Reverse engineering is the process of analyzing a subject system to (i) identify the system's components and inter-relationships and (ii) create representations of the system in another form or at a higher level of abstraction" [12].

In the field of software engineering, developers sometimes do need to understand how existing software works. The concept of reverse engineering, when applied to software leads to many interesting consequences. Various problem areas where reverse engineering has been successfully applied are recovery of design patterns [2], code smell detection [20], re-documentation of programs [6], renewal of user interfaces [36], [38], migration of legacy code [9], translation of program from one language to another [8], and architecture recovery [28].

Reverse engineering has proved very helpful in many ways. But on the contrary, it has lead to many serious problems. "Each year software piracy results in billions of dollars in lost revenue" [11], and hacking is

one of the challenges that reverse engineering has brought into picture (The terms 'hacking' and 'reverse engineering attacks' are used interchangeably in this paper. It refers to the hacking attacks that are based on reverse engineering). "Stealing or replicating someone else's ideas has always been the easiest way of creating competitive products" [26]. The process of reverse engineering helps in understanding the logic of software which makes it easy to alter its behaviour or copy the algorithms. The removal of usage restrictions from software, exploitation of software flaws, cheating in the games and breaking the digital rights of a system are some such reasons for which the hackers resort to reverse engineering [24].

Reverse Engineering Process

"To reverse engineer a software application, it is first necessary to gain physical access to it" [32]. The process of reverse engineering consists of three steps: (i) Parsing and semantic analysis of code, (ii) Extracting information from the code, and (iii) Dividing the product into components, as indicated by Figure 1 [12]. The software code is parsed and semantic analysis is performed on the parsed code. The information thus obtained is stored in an information base and then this information is used to understand the basic functionality and algorithms of the software. This knowledge can be used for legitimate reasons like creating a new system with better design and functionality but practically speaking it can also be misused.

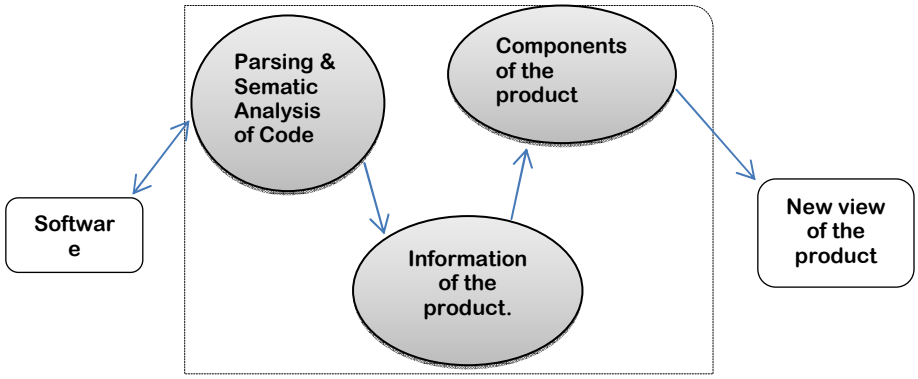


Figure 1 Reverse Engineering Process

Anti-Reverse Engineering

The protective techniques implemented in software in order to protect it from malicious attacks or blatant misuses are referred to anti-reversing techniques. It has become a challenge for the software industry to protect software from attackers and to prevent its misuse. The patent system is not quite as effective with software as it is with traditionally engineered tangible artifacts. While a patent mandates IP protection it is impossible to prove or even suspect any IP theft in a software product that might have been the result of a malicious reverse engineering attack on a patented competitor. After all, such a product, implemented slightly differently from the original, yet using the same core ideas and algorithms could simply be deemed as an inventive step over previous work. [26].

[19] states in his book "It is never possible to entirely prevent reversing" and [11] states "The goal of any "anti" reverse engineering technique is to substantially increase the amount of work that a reverse engineering attempt entails, hopefully beyond the useful lifetime of a software application (or a particular version of the application)". This indicates that it is possible to evaluate the effectiveness of an anti-reversing technique using empirical metrics.

It is not easy to define criteria for evaluating the different reversing techniques.

The criteria that can be used for examining the effectiveness of a reversing technique are [40]:

- Potency – How confused the de-compiler is?
- Resilience – Can it rebuff the de-compilation attempts?
- Cost – How much overhead does it cause?

Anti-Reversing Tools

Reversing is impossible without the right tool [19]. There are various software tools available in the market today; some are free while some cost thousands of naira. The tools available for reverse engineering include de-assemblers available for extracting assembly code from the executables, debuggers for dynamic analysis of code during execution, and de-compilers for generating high-level source code from the executables [11].

The most popular disassembling and debugging tools available include OllyDbg [46], IDA Pro , SoftICE), WinDbg, etc. These tools not only extract the assembly code but also help in viewing many other details of the software. They help in analyzing and patching the code as well.

Java programs are more prone to reversing attacks as "It is more feasible to recover Java source code from Java byte code than it is to recover C/C++ code from machine code" [13]. Just a few of the various decompilers available include Jad [29], JODE [24], and Jdec [5].

A lot of research is going on in the software industry in order to find out successful ways of protecting software from reverse engineering attacks. The techniques proposed to make reverse engineering difficult include obfuscating the code [14], protecting the computing platform physically [17], encryption of executables [11], and watermarking [15].

Java Software: A Direct Threat

The threat of reverse engineering attacks has been taken more seriously since the advent of Java, because the applications written in Java are easier to reverse engineer [13]. To understand why, we have to know the difference between Java byte-code and machine code.

- Machine code or processor instructions are a system of instructions and data executed directly by a computer's central processing unit [34]. These instructions are specific to the processor on which they are generated. Figure 2 illustrates this scenario.
- "Byte-code is a set of instructions that looks a lot like some machine code, but is not specific to any one processor" [31]. "It is the intermediate representation of Java programs just as assembler is the intermediate representation of C/C++ programs" [22]. Figure 3 illustrates the generation of byte-code.

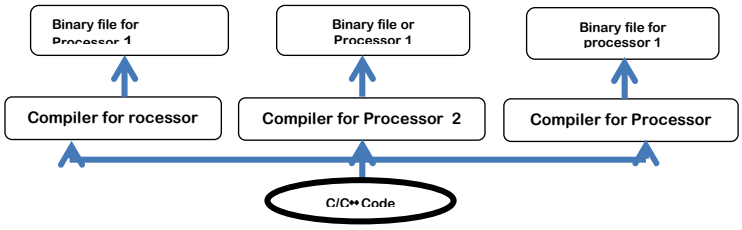


Figure 2: Machine code

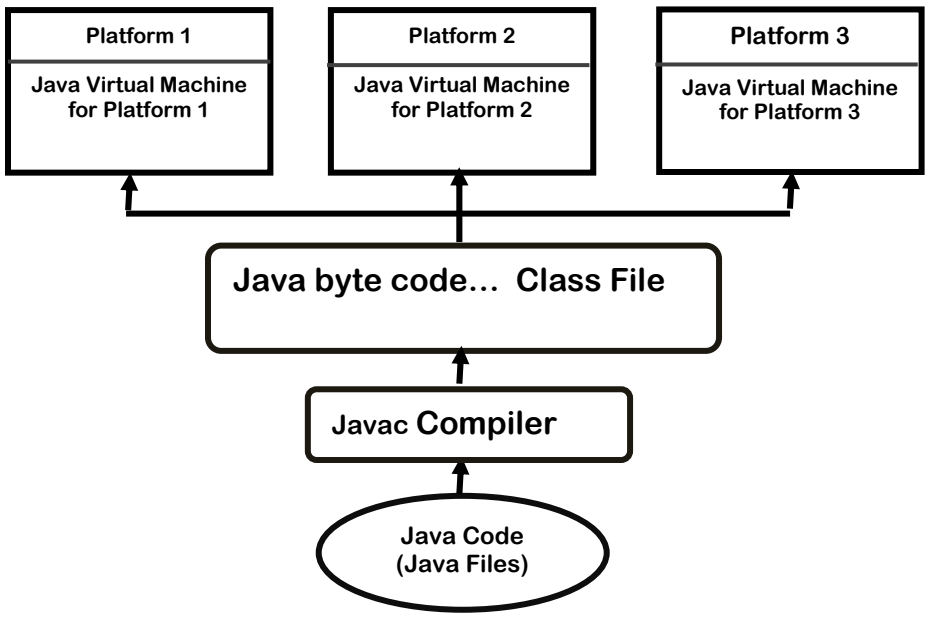


Figure 3: Generation of Byte Code

Java Byte code

Java was designed for supporting platform-independent development. This was done by converting the source code into platform-independent bytecode for compilation. "Java bytecode is standardized and well documented" [26]. It contains a lot of information about the code and thus it can be easily decompiled to the source code. Another characteristic of Java that proves beneficial to the reverse engineering attackers is the use of standard library routines which keeps the size of the application small.

The design of Java language itself, thus, makes it highly prone to reverse engineering attacks. This has become a big problem, as a number of mission critical applications in industries like banking, or simply closed-sourced proprietary applications and games are being developed in the Java language. The purpose of this paper is to analyze the existing anti-reversing techniques that can be implemented to make Java code immune to reversing attacks and suggest a tool that automates the process of implementing anti-reversing techniques for Java software.

Previous Work done

A great deal of work and research has been done in the field of reverse engineering over the past 20 years [10]. Research in the field of reverse engineering had started in the early nineties. Initially, the research was mainly focused on the analysis of procedural software for understanding it and to deal with the Y2K problem (Low, 1998). Architecture recovery was another focus area that was facilitated by reverse engineering. A number of techniques were proposed for component recovery.

Thus, most research during the nineties was focused on three main problems [10]:

- Program Analysis
- Design Recovery
- Software Visualization

The origin of reverse engineering can be traced to software maintenance processes and techniques. The definition of reverse engineering is quite broad today as it encompasses a number of fields like aiding software test by creating representations of code [35], evaluating software design or examining software security [16]. [12] state that the objective of reverse engineering in software is "most often to gain a sufficient design-level understanding to aid maintenance, strengthen enhancements, or support better replacement".

Relationship between Reverse engineering and Re-engineering

Reverse engineering is sometimes understood to be a restructuring technique used for redevelopment of software, which is not precisely what reverse engineering is all about. The objective of the reverse engineering techniques can be broadly classified into two categories: re-documentation and design recovery [10], as shown in Figure 4. "Re-documentation is the creation or revision of a semantically equivalent representation within the same relative abstraction level" [12] and "Design Recovery recreates design abstractions from a combination of code, existing design documentation (if available), personal experience, and general knowledge about problem and application domains" [7].

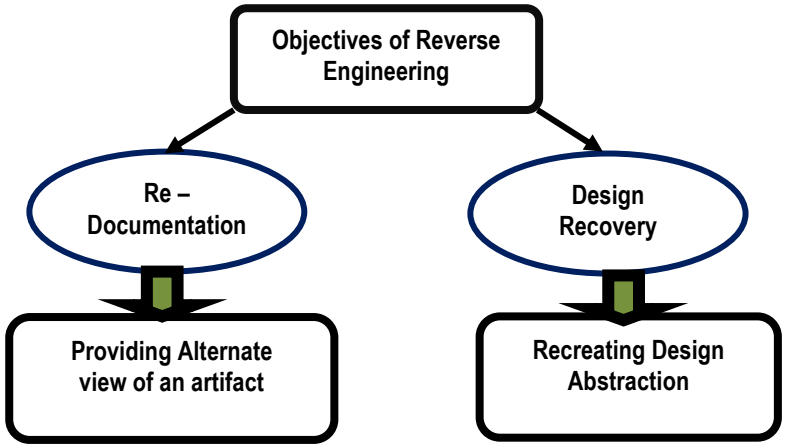


Figure 4 Objectives of Reversing Engineering

The argument given in support of this position is that by definition reverse engineering does not include restructuring or reengineering. Instead, the process of reverse engineering is just a phase of reengineering. Reengineering can be understood as a process with three phases - reverse engineering, architecture transformation and forward engineering. As Figure 5 shows, the reverse engineering phase aims at obtaining an abstraction of the target software and the forward engineering phase aims at the restructuring part.

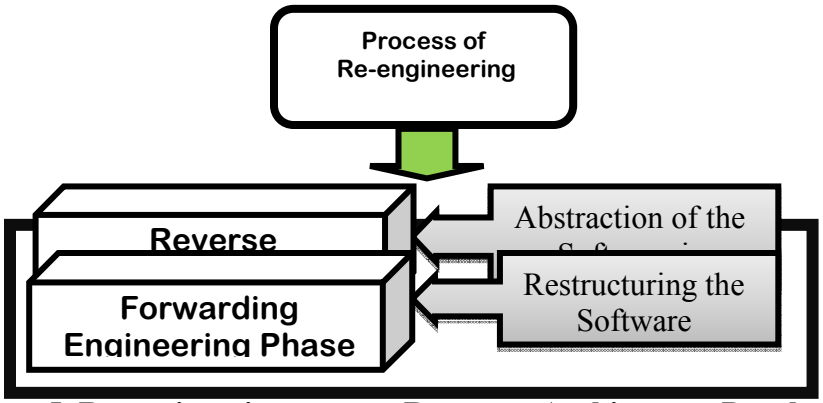


Figure 5. Re-engineering process Recovery Architecture Development

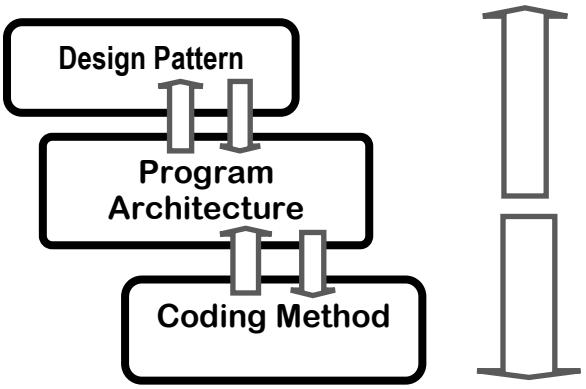


Figure 6. Architecture Re-engineering

Figure 6 presents the Architecture Reengineering process [27]. It indicates that architecture recovery is the reverse process of Architecture Development. For the transformation of software architecture from one form to another, we have to recover the coding approach followed and the architectural plan of the given software. This in turn helps us in figuring out the design patterns implemented in the software. [12] give a clear definition and distinction between the terms reverse engineering, forward engineering, restructuring and reengineering using three software life-cycle stages. The three life-cycle stages that they use are –requirement analysis, design, and implementation. Figure 7 below shows the relationship between the three crucial life cycle stages.

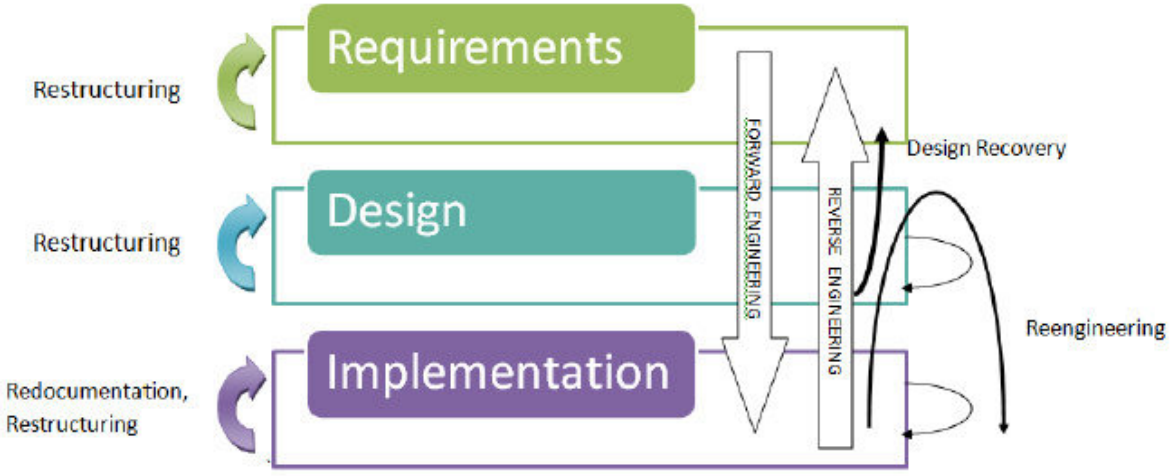


Figure 7 Relationship between the three main life cycles.

Program Analysis

A number of tools have been developed to help in the analysis of computer programs. Initially these tools used static analysis, but eventually this approach was found wanting in many programs where dynamic analysis was required [45]. Dynamic analysis is necessary in many situations and is widely used despite being expensive and incomplete. A number of new analysis techniques have been developed to address the different challenges faced by the software community. For example, the complexity of program analysis increases with program size. So, techniques like island parsing and lake parsing are employed to analyze only small fragments of code at a

time instead of entire programs in one go [37].

Another event that inspired the research effort in the field of program analysis is the presence of clones in software systems [10]. The different techniques developed as an outcome include token-based [3], AST-based [4], and metrics-based [30] techniques.

Architecture and Design Recovery

Initially, the role of reverse engineering in the field of architecture and design recovery was focused on recovering high level architectures from procedural code. With the diffusion of object oriented languages and Unified Model Language (UML), it became important to recover UML models as well from source code.

[43]proposed the static approach for recovering class diagrams and also demonstrated that static analysis was insufficient as it did not contain any information about flow propagation. They successfully extracted sequence diagrams using static analysis on data flow. [45] recovered the UML diagrams by using a combination of static and dynamic analysis techniques.

Another concept that had become very popular along with object-oriented development was design patterns. Recovering the design pattern from the code was helpful in code reuse and assessing code quality. Both static [2] and dynamic analysis techniques [23] were used to recover design patterns.

Visualization

Software visualization is a blessing to the reverse engineers. A pictorial representation of information greatly benefits both the analyzer and the developer. The proper visualization of the program and the information extracted from its analysis is very important for gaining clearer understanding the code. The code flow becomes much easier to understand with a tool that is capable of presenting relevant information at the right level of detail [10]. A number of such tools are available, like Rigi [39], CodeCrawler, Seesoft [18], and sv3D [21].

All these tools provide useful visualization of the software using various techniques. One of these tools, Rigi, can show architectural views, while sv3D can render software architecture metrics in a 3D visual representation. "Code Crawler combines the capability of showing software entities and their relationships, with the capability of visualizing software metrics using polymetric views, which show different metrics using the width, the length, and the colour of the boxes" [10].

These advancements in the field of reverse engineering not only indicate the progress made, but also portray the pitfalls of reverse engineering. With the tools developed for the purpose of helping the software community, another set of people have been benefitted – the hacker community. With so many tools at hand, they can misuse or reuse a lot of licensed software and the algorithms, without paying a dime to the original creators.

What more are we expecting?

While researchers are working on development of more advanced tools to facilitate the process of reverse engineering, in doing so, they are also making the job of hackers much easier. With the advancement in the field of dynamic analysis of programs, hackers can not only analyze their target software statically but can also uncover the exact implementations of its underlying algorithms. The availability of a wide range of efficient de-compilers for high level languages like Java makes it all the more difficult to protect software as it is now possible to recover an almost exact copy of the source code from a class file. And that means copyrights and patents are not very effective. So it is a big challenge for IP owners to protect their code by incorporating anti-reversing techniques into their code.

Anti-Reversing Techniques

To protect Java Code the software development community has been working

on this problem for many years. The techniques that can currently be used to protect Java source code are given in Figure 8 (Nolan, 2004). These techniques are briefly discussed here

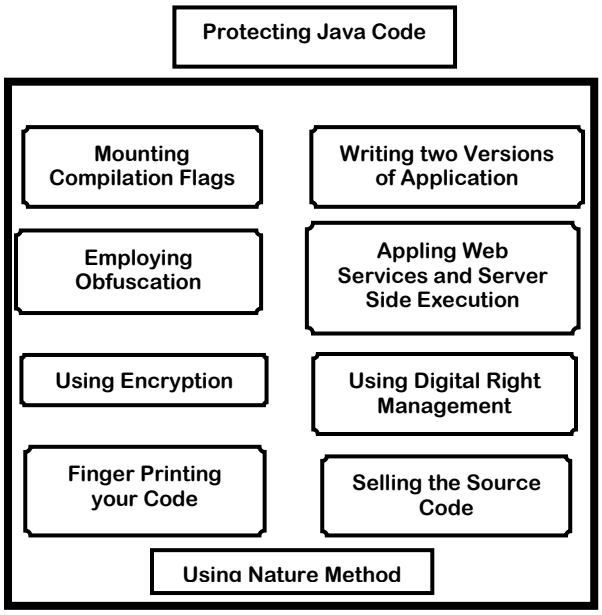


Figure 8 Protecting Java Code

Mounting Compilation Flags

The byte code generated by the compiler is affected by different types of compilation flags [40]. Use of the –g flag during compilation generates debugging tables that contain information about line numbers and local variables [25]. This information is very useful for the decompiler to retrieve the source code.

Implementing Two Versions of the Application

It is a popular trend in the software industry to let users download a fully functional evaluation copy of the software that can be used up to a predefined period of time or a certain number of usages. This introduces the potential threat of malicious users removing these limitations to activate a functional copy of the software without having paid for it after their trial period expired. A possible solution is to implement two versions of the software; with a cut-down trial version that does not reveal all its functionality. Thus the user is forced to buy the original software if they like the trial version. [40]

Applying Obfuscation

Obfuscated code is source or machine code that has been made difficult to understand for humans [41]. There are a number of techniques used to obfuscate code and it is the method used in this paper. The different techniques for obfuscation will be discussed briefly.

Encryption

Throughout the ages, mankind has turned to encryption when trying to protect secret transmissions" [40]. A common solution suggested for preventing the code from de-compilation is to encrypt the class files. These class files are not decrypted until before they are executed.

Digital Rights Management

It is clear from our discussion so far that the bytecode needs to be kept out of reach of the end user in order to prevent them from

decompiling the code. Ultimately, it would be wiser to protect the code by simply securing the browser and class loader using a trusted browser. The browser should not let the end user access the cache which contains code. [40]

Fingerprinting the Code

Digital fingerprinting is a string of binary digits that uniquely identifies a file and it is usually in the form of a copyright notice that helps you to identify your code. Inserting a fingerprint does not provide any protection but it helps in protecting the copyright by providing a way for the developer to prove that the code was originally written by him. [40]

Selling Source Code

"If source code is so readily available, then why not just sell it at a higher price?" [40]. The de-compiler can be discouraged to decompile if you sell the source code directly to him.

Employing Native Methods

As we said earlier code written in Java is more difficult to protect than that written in C/C++. [40] suggests that we can protect our Java code by compiling it in C or C++. It is possible to do this in Java by using the Java Native Interface (JNI). It might cause portability issues but is useful if portability is not an issue.

Obfuscation Techniques

There are a number of techniques that can be used to make software immune to reversing attacks. Many of these techniques are used by the obfuscators available in the market. These various obfuscation techniques can prove beneficial in protecting Java software from reversing attacks.. Obfuscation can be classified into three classes:

Source code obfuscation: The obfuscation is performed on the source code.

Bytecode obfuscation: The transformations are performed on the bytecode of the compiled software.

Binary code obfuscation: The obfuscation is achieved by rewriting the instructions at machine code level.

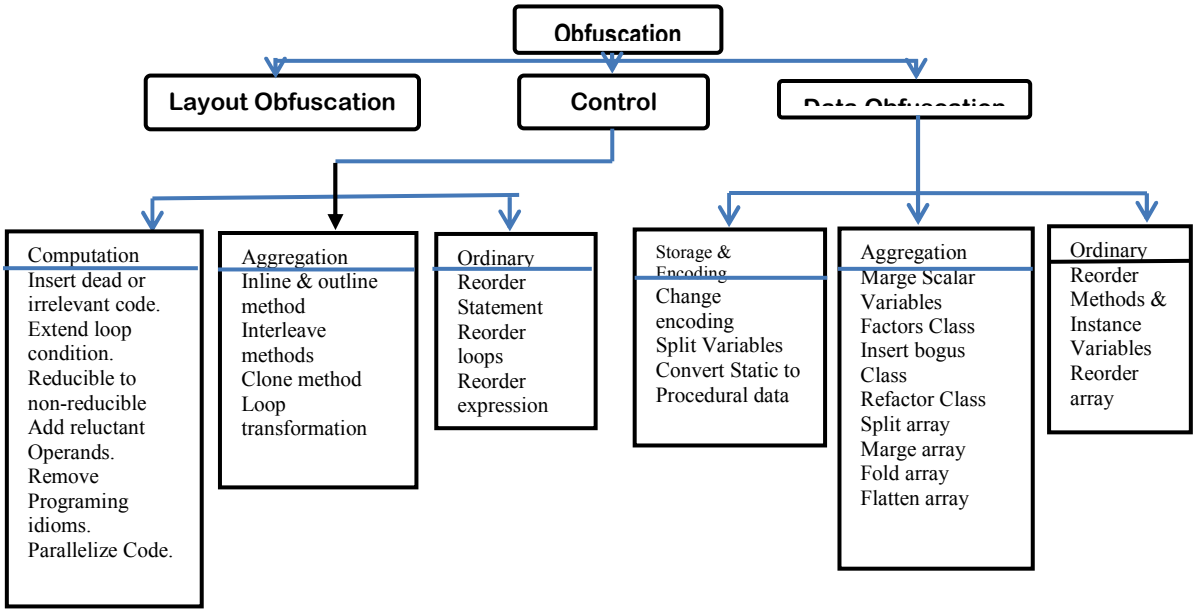


Figure 9 gives another classification of the obfuscation techniques [40], [14] based upon how the code is obfuscated.

Obfuscators available in the market work by scrambling the identifiers in the classfile to make the decompiled source useless. The variables are renamed with automatically generated garbage variables which do not affect the code functionality as the class file uses pointers to methods and variables instead of actual names. It becomes difficult to understand the code but it is not impossible. A dis-assembler can be used to rename the variables in order to generate more meaningful names. [40]

Novel Framework Technique.

Applying anti-reversing techniques is a complex procedure. It involves detailed scrutiny of the code, extracting information about its design, and making changes to the data and control flow without altering the program logic. Our tool is code named **KDefender**, automates a number of obfuscation techniques. The automation of all the techniques is very difficult because of their complexity and limitations of the implementation language. Manual application of all the techniques is not feasible as it is time consuming and becomes unmanageable with increase in the program size and complexity.

KDefender Functionality

Let us briefly outlines the functionality and features provided by KDefender. The tool analyzes Java code and applies various obfuscation techniques to the code to make it harder to reverse engineer. KDefender is a relatively small tool that uses an ANTLR [1] generated parser to parse the input Java source code. "ANTLR (ANother Tool for Language Recognition) is a language tool that provides a framework for generating parser from grammatical descriptions" [1]. As a proof of concept for our findings, KDefender was tested on a single Java file at a time and generates an obfuscated output that is remarkably difficult to reverse engineer. It can be easily modified and extended to obfuscate an entire project containing several Java source files.

Techniques Implemented by KDefender

The KDefender code itself uses the data structures and then works based on the information generated by the parser. KDefender applies the following obfuscation techniques to a Java program: (All the obfuscation techniques implemented by KDefender are adopted from suggestions made by [14] and [40] See figure 9

Layout Obfuscation

Scramble identifiers

Control Obfuscation

Insert dead or irrelevant code; Extend loop condition & Add redundant operands

Data Obfuscation Insert bogus class; Reorder methods & Convert static to procedural data

The algorithms for implementing each one of these obfuscation techniques are briefly discussed below

Control Obfuscation

The idea behind control obfuscation is to disguise the real control flow [32]. The control flow of the source code is altered to confuse anyone looking at the decompiled code [40]. [26] states, "The best obfuscators are capable of transforming the execution flow of bytecode by inserting bogus conditional and goto statements". [14] classifies control obfuscation into three different categories – computation, aggregation, and ordering. Complicating the loop conditions introduces obfuscation in the code. This can be done by extending the loop condition with a second or third condition that doesn't do anything [40]. For example, in the following example we have a simple if condition.

Before:

```
int x = 1;
if (x > 200)
{
…
x ++;
// call function abc(x)
}
```

After:

```
int x = 1;
while (x> 200 || x%200==0)
{
…
x ++;
// call function abc(x)
}
```

This condition is easy to understand as it has no calculation involved. But if we replace this code with condition that does the same job but looks complex, it might make it a little more time consuming for an attacker to understand the logic.

Reducible to Non-reducible

The Holy Grail of obfuscation is to create obfuscated code that cannot be converted back into its original format" [40]. We can devise some transformations that make the code non-reducible to its original form. For example, the Java bytecode has goto instruction while no equivalent statement exists in the Java language. So, the flow graphs produced from Java programs are always reducible, while those from Java bytecode may express non-reducible flow graphs. Expressing non-reducible flow graphs is inconvenient in Java due to unavailability of goto statements, so we need to do some transformation for converting the reducible flow graph into a non-reducible one. We can achieve this by converting a structured loop into a loop with multiple headers [14]. For example, see the code below:

Before:

```
Statement 1;
while (condition1)
{
Statement2;
}
```

After:

```
Statement 1;
if(condition2)
{
Statement2';
while (condition1){
Statement2;
}
else {
while (condition1){
Statement2;
}}

else {
while (condition1){
Statement2;
}}
```

In this algorithm, we had a simple while condition. We split the statement to make it appear more complicated than it actually is.

Add Redundant Operands

Adding some insignificant terms to the code, in the basic calculations confuses the reverse engineer. For example, let"s assume that there is an integer variable, „p" that

stores the product of two integer variables – „a" and „b". The code below shows we can make the calculations look complex to the attacker. [40]

Before:

```
public int sum{
int a = 5;
int b = 7;
int p;
p = a * b;
System.out.println("
Product =" + p);
}
```

After:

```
public int sum{
int a = 5, b = 7;
double i = 0.0005;
double j = 0.0007;
double p;
p = (a * b) + (i*j);
System.out.println("
Product =" + (int) p);
}
```

Both of these code snippets will generate exactly the same output, just that the second one looks more complex than the original one. [40] warns that using this technique all through the application has the potential to degrade its performance.

Framework Implementation

KDefender is implemented in C# and uses an ANTLR generated parser [1] for parsing the program. The IDE used for development is Microsoft Visual Studio.Net. The tool applies all the obfuscation techniques in one step and gives the option of reviewing the code before it is saved. The input and output are both Java source code. As mentioned above, the tool uses various data structures for implementing different obfuscation techniques.

KDefender implements maximum number of obfuscation techniques as compared to any other tool on the market. All the tools on market implement different set of techniques while KDefender provides a prototype for a tool that implements most of these techniques in one place. KDefender makes the Java code difficult to reverse engineer by applying various obfuscation techniques. The techniques that can be implemented to enhance the tool are mentioned in this paper. It is left as future work to enhance the capabilities of the tool to make it a commercially useful tool

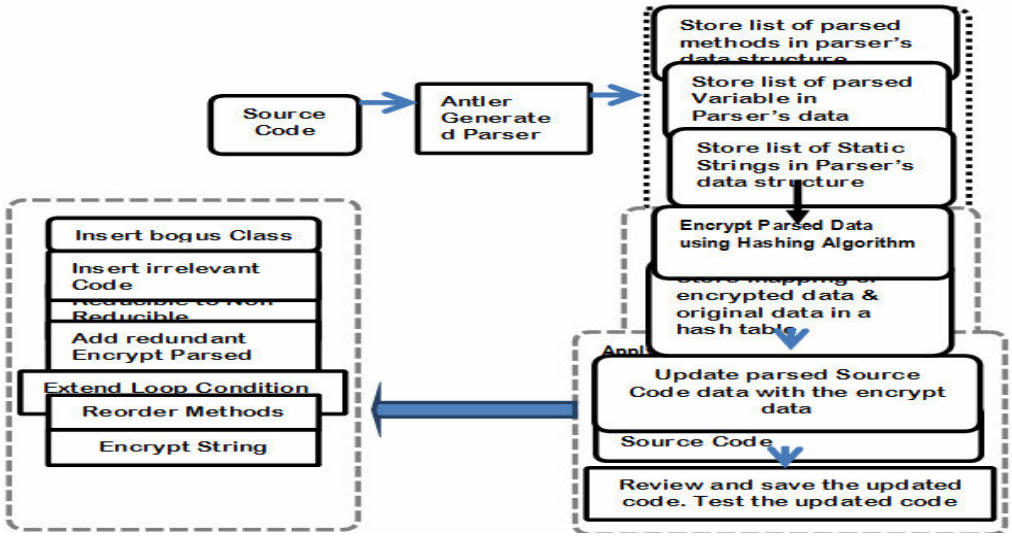


Figure 10: KDefender Implementation

Conclusion

With the availability of so many advanced tools and techniques, Java programs are vulnerable to reverse engineering attacks. The research described in this paper has lead to the creation of a new tool to automate the application of strong anti-reversing techniques to Java programs. This effort can go a long way in addressing the problems of unauthorized access to source code and IP theft using reverse engineering attacks that the industry currently faces it might very well be impossible to eradicate it but our tool can surely make the reverse engineering effort hard and practically worthless.

In this paper, we presented the different techniques that are helpful in protecting Java software from reverse engineering attacks. We discussed the different obfuscation techniques previously developed. We identified the techniques that could be automated and then developed a prototype to demonstrate the automated application of these techniques.

The obfuscation can be applied to the java source code files and our tool generates an obfuscated version of the code as its output.

Recommendation

The current prototype of KDefender works on one Java source file at a time. A full version could be easily created by enhancing the prototype and that would work on an entire project containing several Java files.

Our framework implements several obfuscation techniques in total. Further research based on this ground work would lead to automation of even more techniques and in fact, development of more advanced techniques based on future needs.

Needless to say, if all the known obfuscation techniques could be automated, it would make this tool even more powerful

.

References

[1] ANTLR (n.d.) Retrieved from the ANTLR website: http://www.antlr.org/

[2] Antoniol, G., Casazza, G., Penta, M.D., & Fiutem, R. (2001). Object-oriented design patterns recovery, Journal of Systems and Software, Volume 59, Issue 2,

[3] Baker, B.S. (1995, July). On finding duplication and near-duplication in large software systems. In proceedings of the Working Conference on Reverse Engineering.

[4] Baxter, I.D., Bier, L., Moura, L., Sant‟‟Anna, M., and Yahin, A. (1998). Clone detection using Abstract Syntax Trees. In *Proceedings of the International Conference on Software Maintenance*, pages 368-377

[5] Belur, S. & Bettadapura, K. (2006). *Jdec: Java Decompiler*. Retrieved November 20, 2010 from: http://jdec.sourceforge.net/

[6] Benedusi, P., Cimitile, A., & Carlini U.D. (1992, November). Reverse engineering processes, design document production, and structure charts. Journal of Systems and Software, Volume 19, Issue 3,

[7] Biggerstaff, T.J. (1989, July). Design Recovery for Maintenance and Reuse. IEEE

Computer Business Software Alliance (May 2008). Fifth Annual BSA and IDC Global Software Piracy Study. Retrieved on February 2, 2011 from BSA website:

[8] Byrne, E. (1991). Software reverse engineering. Software – Practice and Experience, 21(12):1349-1364.

[9] Canfora, G., Cimitile, A., Lucia, A. De, & Lucca, G. A. Di (2000). Decomposing legacy programs: a first step towards migrating to client-server platforms. Journal of Systems and Software, 54(2):99-110. 84

[10] Canfora, G. & Di Penta, M. (2007, May). New Frontiers of Reverse Engineering. In *2007 Future of Software Engineering* (May 23 - 25, 2007). International Conference on Software Engineering. IEEE Computer Society, Washington, DC,

[11] Chen, Y., Fu, B., & Richard III, G. (2006, March). Some New Approaches For Preventing Software Tampering. *ACM SE'06* March 10-12, Melbourne, Florida, USA

[12] Chikofsky, E.J.; Cross II, J.H. (1990). Reverse Engineering and Design Recovery: A Taxonomy in IEEE Software [Electronic version]. *IEEE Computer*

[13] Cipresso, T. (2009). Software Reverse Engineering Education. *Master's thesis*, San Jose State University, CA. [Electronic version] Retrieved December 3, 2010, from Software Reverse Engineering (SRE) – Web supplement

[14] Collberg, C., Low, D., & Thomborson C. (1997). A Taxonomy of Obfuscating Transformations. *Technical Report.* Department of Computer Science, University of Auckland, New Zealand. Retrieved October 21, 2010

[15] Collberg, C. & Thomborson, C. (2002). Watermarking, Tamper-Proofing, and Obfuscation – Tools for Software Protection. IEEE traction on software engineering 8(28), pages 735- 746

[16] DaCosta, D., Dahn, C., Mancoridis, S., & Prevelakis, V. (2003). Characterizing the „security vulnerability likelihood" of software functions. In ICSM, pages 266-275. IEEE Computer Society.

[17] Doorn, L.V., Kravitz, J., & Safford, D., (2003). Take control of TCPA, Linux Journal. [Electronic version] Volume 2003 Issue 112. Retrieved October 31, 2010 from http://www.linuxjournal.com/article/6633

[18] Easterbrook, S.M., Holt, R.C., and Elliot Sim, S. (2003). Using benchmarking to advance research: A challenge to software engineering. In *proceedings of the 25th International Conference on Software Engineering* (ICSE 2003), May 3-10, Portland, Oregon, pages 74-83

[19] Eilam, E. (2005). *Reversing: Secrets of Reverse Engineering*. Indianapolis, Indiana: Wiley Publishing, Inc.

[20] Emden, E.V. & Moonen, L. (2002, November). Java quality assurance by detecting code smells. In Ninth Working Conference on Reverse Engineering (WCRE 2002), Richmond, VA, USA, pages 97-107. DOI:10.1109/WCRE.2002.1173058

[21] Feng, L., Maletic, J.I., and Marcus, A. (2003). Source Viewer 3D (sv3D) – a framework for software visualization. In *proceedings of the 25th International Conference on Software Engineering* (ICSE 2003),

[22] Haggar, P. (2001). Java bytecode: Understanding bytecode makes you a better programmer. [Electronic version] Retrieved October 21, 2010 from http://www.ibm.com/developerworks/ibm/library/it-haggar_bytecode

[23] Heuzeroth, D., Holl, T., Högstorm, G., and Löwe, W. (2003). Automatic design pattern

detection. In *11th International Workshop on Program Comprehension* (IWPC 2003), Portland, Oregon, USA, pages 94-103

[24] Hoenicke, J. (2002). *JODE – Decompiler and Optimizer for Java*. Retrieved November 20, 2010, from http://jode.sourceforge.net/

[25] Javac – The Java Compiler (n.d.). The Java(tm) Tools Reference Pages. Telemedia, Networks, and Systems Group, MIT Laboratory for Computer Science, Cambridge, MA. Retrieved December 29, 2010 from Telemedia, Networks, and Systems Group‟s website:

[26] Kalinovsky, A. (2004). Covert Java: Techniques for Decompiling, Patching, and Reverse Engineering. Bedford, UK: Sam Publications

[27] Kazman, R., Woods, S. S., & Carri`ere, S. J. (1998). Requirements for integrating software architecture and reengineering models: Corum II. *In Proceedings of the Working Conference on Reverse Engineering*, pages 154–163

[28] Koschke, R. (2000). Atomic Architectural Component Recovery for Program Understanding and Evolution. *Ph.D. thesis*, University of Stuttgart, Germany.87

[29] Kouznetsov, P. (1997). Jad – *the fast Java de-compiler*. Retrieved December 3, 2010,

[30] Leblanc, C., Mayrand, J., and Merlo, E. (1996). Experiment on the automatic detection of function clones in a software system using metrics. In *Proceedings of the International Conference on Software Maintenance,* pages 244-253, Monterey,CA

[31] Lemay, L. & Perkins C.L. (1996). Teach Yourself JAVA in 21 Days. Indianapolis, Indiana: Sams.net Publishing, Inc.

[32] Low, D. (1998). Java Control Flow Obfuscation. Master‟s thesis. University of Auckland, Auckland, New Zealand.

[33] Low, D. (1998). Protecting Java Code Via Code Obfuscation. ACM Crossroads, Spring 1998 issue. Retrieved from The University of Arizona website on June 30, 2010:

[34] Machine code (2010). Wikipedia. Retrieved December 4, 2010, from http://en.wikipedia.org/wiki/Machine_code

[35] Memon, A.M., Banerjee, I., & Nagarajan, A. (2003). GUI ripping: Reverse engineering of graphical user interfaces for testing. In Tenth Working Conference on Reverse Engineering (WCRE 2003), 13-16 November, Victoria, Canada, pages 260-269

[36] Merlo, E., Gagne, P.-Y., Girard, J.-F., Kontogiannis, K., Hendren, L.J., Panangaden, P., & Mori, R. de (1995). Reengineering user interfaces. IEEE Software, 12(1):64-73

[37] Moonen, L. (2001). Generating robust parsers using island grammars. *In Proceedings of the Working Conference on Reverse Engineering*, pages 13–22 88

[38] Moore, M. (1998). User Interface Reengineering, *Ph.D. thesis*, Georgia Institute of Technology, USA

[39] Muller, H.A., Storey, M.D., Tilley, S., and Wong, K. (1995). Structural re-documentation: A case study. IEEE Software, pages 46-54

[40] Nolan, G. (2004). *Decompiling Java*. Chapter 4 – Protecting Your Source: Strategies for Defeating Decompilers, pages 79 – 210. New York, USA: Springer-Verlag New , Inc.

[41] Obfuscated code (2010). Wikipedia. Retrieved November 4, 2010, from http://en.wikipedia.org/wiki/Code_obfuscation

[42] Parr, T. (2007). The Definitive ANTLR Reference. Building Domain-Specific Languages. The Pragmatic Programmers, LLC

[43] Potrich, A. and Tonella, P. (2005). Reverse Engineering of Object Oriented Code. Springer-Verlag, Berlin, New York
[44] Stamp, M. (2006). *Information Security: Principles and Practices*. New Jersey: John Wiley & Sons, Inc. 89
[45] Systä, T. (2000). Static and Dynamic Reverse Engineering Techniques for Java Software Systems. PhD thesis, University of Tampere, Finland
[46] Yuschuk, O. (2000). *OllyDbg*. Retrieved December 3, 2010, from http://www.ollydbg.de/

Technology Management in Services: Understanding Sources of Value Creation and Service Output Characteristics

[1]Rasheed A. Raji, [2]Babatunde B. Olofin, & [3]Oladimeji, S. A.

[1]Department of Computer Science, Federal Polytechnic Damaturu, P O Box 358, Damaturu, Nigeria
[2,3]Department of Computer Science, Federal Polytechnic Nekede, P O Box 4545, Enugu, Nigeria
[1]Cell: +2348061596436; Email: rajiayanda@gmail.com. [2]Cell: +2348033215972; Email: bbolofin@gmail.com
[3]Cell: +2347030623266; Email: dimejibiodun@hotmail.com

Abstract

Technology has had a profound effect on how services are designed and delivered. We have seen many changes emerging in services as a result of technology. A survey of the existing classification schemes of services shows that they are not designed specifically for the management of technology in services, and, thus, falls short when applied to such an environment. This paper presents the argument that a classification scheme, which incorporates the idea of the source of value added and the degree of product component delivered, offers an effective method of classifying services for the management of technology. This paper also explores the strategic technology management issues on different types of service.

Keywords: *Customer value, Service characteristics, Service Classification, Service technology, Technology management*

Introduction

In recent years, much has been written about the growth and importance of the service sector. As this area of the economy has grown, the role of technology as a source of building competitive advantage has been critical. For nearly a decade, students of the service sector have been exploring the relationship between technology and competitive advantage of service sector [1, 2, 3, 4, 5, 6, 7, 8, 9]. We have also seen many changes emerging in services as a result of technology. Numerous examples of technological advances in banking [6][8]; health care [10]; professional service [11][2][13] and education [14][15] [16] have been central to industry- wide growth and the creation of new markets. For example, Ernst & Young offers continuing education to its national workforce through a private satellite network. A cost- and time-effective alternative educational delivery system provides tremendous opportunities to educate both internal staff and the firm's clients, and almost eliminates non-billable travel time and travel costs. American Airlines created distinctive competitive advantages through differential expertise using Sabre system and SMARTS over the years. Merrill Lynch's Cash Management System, based on a Banc One information system that integrated a variety of customer accounts, gave the company an enormous and sustainable market share advantage over fast following competitors that offered similar services. FedEx solidified its competitive standing with a system for tracking the status of customers' packages in real time. Citibank

dramatically increased its market share in retail banking in part through the introduction of automatic teller machines well before its competition. Over time, it has become increasingly critical for firms in these and other service industries to effectively manage the use and adoption of critical technologies.

The differences between different types of services have presented a particular difficulty for researchers attempting to offer prescriptive advice regarding effective management practices. Because of the broad range of service types, researchers in the area have worked todevelop methods of classifying services in a number of ways: the nature of the service product [17, 18], the view of the service recipients [5], 19, 20], the standpoint of the main producer of the service products [21], synthesized classification [22, 23] and the time and space utility creation [24]. These classification schemes have been useful in providing insight into effective management practice. However, developing classification schemes is not enough. If they are to have managerial value, they must offer strategic insights. While these classification schemes provide useful guidance from many perspectives, they were not designed explicitly to be applied to technology management in services. Therefore, they often have their shortcomings. For example, estimating the degree of customer contact provides little guidance on effective technology implementation practices in banking. That is why it is important to develop ways of classifying services that highlight the characteristics they have in common, and then to examine the implications for technology management. This paper presents the argument that a conceptual framework, which incorporates the idea of the source of the value added and the degree of product component delivered offer an effective method of classifying services for the management of technology.

In the text below, we begin by providing an overview of several of the popular classification schemes of services. We then outline the important role of technologies in service. Finally, we outline the utility of existing frameworks of services and present the argument for the new perspective as an effective means of managing technologies in services.

Characteristics and Classification Of Services

Early research in the field sought to differentiate services from standard manufacturing environments in a number a ways; focusing particularly on four generic differences- intangibility, heterogeneity, perishability of output, and simultaneity of production and consumption [17, 25, 26, 27, 28, 29, 30, 31]. Although these characteristics are still commonly cited, they have been criticized as too generic to understand the processes underlying service delivery [32, 33, 34, 35]. There is a growing recognition that they are not universally applicable to all services. Lovelock and Yip [35] provide an alternative set of eight characteristics. These characteristics begin with the nature of the output-performance rather than an object. This include customer involvement in production, people as part of the service experience, greater likelihood of quality control problems, difficulty in customer evaluation, lack of inventories for services, greater importance of the time factor, and availability of electronic channels of distribution. These characteristics provide a useful starting point for thinking about the distinctive aspects of service management.

From an operational perspective, Lovelock and Yip [35] assign core services to one of three broad categories (people-processing, possession-processing, and information-based services), depending on the nature of the process and the extent to which customers need to be physically present during service production. People-processing services

involve tangible actions to customers in person. These services require that customers themselves become part of the production process, which tend to be simultaneous with consumption (i.e., passenger transportation, health care, food service, lodging services). Possession-processing services involve tangible actions to physical objects to improve their value to customers (i.e., freight transport, warehousing, equipment installation and maintenance, car repair, laundry, and waste disposal). The object needs to be involved in the production process, but the customer does not, since consumption of the output tends to follow production. Finally, information-based services involve collection, manipulation, interpretation, and transmission of data to create value (i.e., accounting, banking, consulting, education, insurance, legal services, and news). In production of information-based services, customer involvement is often minimal.

The core service product is typically accompanied by a variety of supplementary service elements (i.e., order taking, billing, and payment), which, taken together are commonly referred to as the "service bundle". These supplementary elements not only add value, but also provide the differentiation that separates successful service providers from the rest.

According to Thomas [21], the traditional perspective of the service business that the service is "invariably and undeviatingly personal, as something performed by individuals for other individuals" is erroneous. Automatic car washes, automated banking services, and computer time-sharing are just three examples of the many service businesses in which the service is primarily delivered through interactions with automated equipment [36], [37]. The strategic requirements for these businesses are obviously quite different from those in which individuals perform services for other individuals. Thomas suggests one way to separate service businesses into general types (equipment-based and people-based service), according to different strategic management requirements. According to Thomas [21], to effectively manage a specific service business, it is necessary to answer two questions: (1) how is the service rendered? (2) What type of equipment or people renders the service?

Thomas argues that service business managers can analyze their companies and take advantage of the strategies that are uniquely available to them. Also, based on the above classification of service type, management in service businesses can better understand the nature of the strategic opportunities of their firm's position. As will be seen later, the model we present for the management of technology in services builds on these ideas of Thomas, expanding on and refining the equipment/people based idea and incorporating issues specific to technologically rich environments.

In summary, a survey of the existing classification schemes of services shows that they are not designed specifically for the management of technology in services, and thus falls short when applied to such an environment.

Technology Management In Services

Technology as a source of building competitive advantage is playing an important role in many service industries. Service technologies typically are described as "knowledge technologies" [38], [39], and defined by Dubin [40] as "the body of ideas which express the goals of the work, its functional importance, and the rationale of methods employed." Implementing technology in service environments creates many difficulties for the firm, as traditional manufacturing-based methods may not be appropriate. According to Mills and Moberg [41], this is because applying "the manufacturing transformation process model" (in which raw materials are processed and can be put into inventory as finished goods waiting

for customer demand) to service operations is problematic. Since services cannot be stored, one is forced to conceive input and output sectors as depositories of client/customers waiting for entry on one hand and exit on the other hand. The conversion is restricted to the direct interaction between client/customer and service worker. Yet, this neglects several important features of service operations. First, technologies may be employed outside the conversion (interaction) process itself. Thus, technology is applicable at all stages of the service production system not just within the so-called conversion process. Second, the transactional nature of the interaction within the conversion processes invites recycling, skipping, and aborting. Thus, the conversion process may be composed of several typical information-exchange sub-processes, but these constitute a reciprocal rather than a linear sequence. Third, because of the interactive nature of many services, unintended or serendipitous conversions may occur at any stage in the system. Client/customers may experience insight, inspiration, or even instantaneous learning with the workflow. In sum, the distinction among inputs, conversion, and outputs is muddied in the service production process and it often bears little resemblance to a strict production environment.

The split between manufacturing and service-based industries often has far reaching effects. In a discussion of the diffusion of new technologies in services associated with 'technology push' and 'demand pull' processes, Barras [42] outlines the familiar 'product cycle' theory of innovation, whereby successive waves of innovation in a particular technology shift progressively from product innovations which generate new devices to process innovations which improve the quality or performance of existing devices. However, based on an empirical study of the adoption of information technology in service industries, Barras suggests that an opposite process of innovation tends to operate, which can be termed a 'reverse product cycle'. Thus even the very nature of the evolution of product and process development may be different. The context within which knowledge technologies are brought to bear on client problems also is different [25]. To produce a service, the customer and service worker must interact for the delivery of the service to be complete [43]. Thus, the client/customer and service worker exchanges information and commitment ('Transaction Process' in Thompson). The necessary contact between client/customer and service worker has several other implications. First, the spectrum of customer reactivity is a striking outcome of many interactions. Second, service technologies require a high capacity for information processing within the technical core. Finally, service technologies depend on the client/customer not only to provide the information that constitutes the raw material to be worked on, but also often to make use of client efforts in the service production process [14]. This means that client/customer is involved directly in the production of his/her own wants.

Thus, in summary, service operations seem to have several features that distinguish them from manufacturing. These emerge from the intangibility of service outputs and the peculiar nature of service technologies and the service process, including perishability. Unfortunately, there is not much to be learned regarding technology implementation in services. Thus firms are left with no choice but to follow guidelines established in manufacturing settings found in the existing literature.

As it was noted earlier on, researchers have tried many ways of "splitting up" the service sector because of the wide breadth and diversity of services in existence [32, 33, 20, 21, 22, 23, 27, 28, 34]. Services vary significantly across a number of dimensions, and this must be managed differently in different scenarios. One

would not expect to find "universal" approaches to the effective management of every type of service. Technology - viewed as encompassing skills, expertise, know-how, and the organization of work- has become a major competitive weapon in service sectors [44, 45, 5, 23, 26, 46, 47, 48]. To gain a competitive advantage, technology is often implemented in ways that yield improvements in the bundled end product. As in other management practices, the process of implementing a new technology in services differs significantly from industry to industry within the sector. In some types of services, the product, the production process, or both, have a significant dependence on the implementation of an advanced technology. Digital computers, for example, have become integral to the production of new types of services (i.e., data processing itself and computer-assisted architectural drafting). In these environments, however, computers are used to enhance people's skills rather than replace them entirely. The operator (a draftsman) still needs basic skills and knowledge of drafting in order to use the computer-assisted equipment effectively. Such a technology might render some skills obsolete (drawing, lettering, …), but at its core, the technology is designed to enhance an operator existing knowledge base.

In another service environment, advanced technologies may have a prominent place in the product/process environment in such a way such that it reduces the required skill set of the operator, instead embedding some of the skills and knowledge into the equipment itself. Consider for example, the adoption of automated cooking equipment at a fast food restaurant. The technology adoption here would affect the core of the "value added" in the service bundle rather than enhance the operators skills,. Thus, it is the technology that provides the value-added, rather than the worker. For example, since 1990, Arby's has been installing automated systems for food selection and payment as part of its plan to revolutionize customer service. The roast beef sandwich chain is using Touch 2000, a computerized system that allows customers to order food from a touch-sensitive display screen, processes the information through an IBM PS/2 Model 30 computer, and displays it on IBM monitors in the food preparation area. The chef, while working within a service operation, uses the technology (i.e., an automated french-fry cooker) to deliver a bundled service to the customer. In such environments, the competencies of the technology itself go a long way in creating the competitive advantage.

As it can be seen from these examples, technology implementation in services in which a considerable amount of the value-added comes from the worker him/herself is different from those where the value-added is in the equipment. The implementation process in such environments differs greatly. For example, worker buy-in and feedback would be more critical where the technology is enhancing worker skills. Even the rationale for implementing the service in the first place would be quite different. Fischer [13] studied new audit technology adoption in CPA firms, where the technology serves to enhance the knowledge and skills of the accountant. He found that the benefits of new technology in this particular service sector did not result directly from the adoption and use of the new technology. Rather, these benefits resulted from the concomitant reduction or elimination of other audit procedures that had been performed in the past. The core tenets of Advanced Manufacturing Technology (AMT) adoption literature [49] may not be appropriate in these environments because the portion of the service which is knowledge based is inherently tacit, difficult to measure and difficult to transfer. The quality of the service is not "conditioned into the consumer", and the

professional will stand or fall with the perception of the customer. The result is that the quality of the service is not as routinized. New technology acceptance in these cases is at the discretion and description of the individual distributing it. The abilities of the individual delivering the service will ultimately drive its final quality. In addition, while service outcomes in these areas can often be measured through traditional quality measures, the customers' perception of the service outcome may vary considerably over time.

Additionally, services can vary significantly in the amount of physical product delivered
in the bundle. Those with a significant product component behave differently than those where a "pure" service is delivered. In "pure" services, the degree of customer contact is often higher, and perceptions play a greater role [50]. In services with a significant product component ("goods-like"), traditional methods of controlling quality might come into play. For example, some restaurants (i.e., Diners) have poor or even rude service, but thrive because of the high quality/value of the food delivered. While this distinction has been made in previous research (and thus will not be elaborated on here), it remains central to effective technology management in the service sector.

Service Classification

Sources of Customer Value

As the above discussion outlines, in technology management in services, it is useful to divide the service sector according to the utilization of those services that have the majority of knowledge embedded in the service production system (i.e., fast food, automated car wash, broadcasting, theatres, and museum) versus those services which are based on the knowledge of the point person providing the service (i.e., teaching, exercise clinics, computer graphic, professional consulting, and legal services). We classify *Knowledge-based Services* as those services in which the majority of customer value is provided by the knowledge of the person providing the service. We classify *Knowledge-embedded Services* as those services that embed the customer value in the system that provides the service. As was noted earlier, existing classifications of service business (i.e., [21, 23, 24, 35]) do not show the process and/or mechanism of customer value creation. In view of the important relationship between customer value and service, this perspective focuses on how customer value is created, what mechanisms are utilized in "value-added", and how competence in service can be enhanced. An important difference is that this framework focuses on where the "value added" comes from, rather than what the process "looks like".

Characteristics of Service Output

Services can be classified according to the extent to which physical product is incorporated within the output. Those services which have a substantial product component ('*Goods-like' Services*) are quite different from those which do not ('*Pure' Services*). In the technology adoption and implementation phase, a service, which has a significant product component, may, in many ways, behave like a production environment. For example, the similarities between a production facility and the flow of product through a fast food service provider are obvious. As such, many issues (such as type and method of employee training and empowerment) learned through technology implementation in a production environment would be applicable here. Furthermore, the driving reasons behind technology adoption in this service with a significant product component might again resemble those found in a production environment: efficiency, conformance quality, flexibility, yield, etc. Contrast this with a more "pure" service, where the technology will most likely interact

directly with the customer, as opposed to those occurring "behind the scenes", (i.e., call waiting, pay-per-view movies); these technologies are more often implemented to directly provide the customer with new features and capabilities, and are less concerned with production.

Table 1: A Classification of Services

Type I: Knowledge-based 'Goods-like' Services

Consider for example, the implementation of highly sophisticated computer graphic equipment (hardware and/or software) in a firm that provides computer graphic design services for art, publication, video production, and presentation. While computer graphic equipment is a powerful tool, the technology is typically aimed at enhancing the existing skills and capabilities of the design workforce, rather than replacing it. Adopting the state of the art graphic design system does not eliminate the need for workers with knowledge and training in structural design. Rather, the technology enables the user to gain benefits such as increased speed (efficiency), the ability to create a "library" of designs to be re-used (repeatability), and increased accuracy of drawings (quality). This reflects the fact that this service has a significant product component— the drawing itself. As will be seen in later examples, the above mentioned goals are not shared with technologies implemented in pure services.

Since the primary "value-added" of the computer graphic service remains in the hands of the designer, we would classify this as a knowledge-based service. As such, the choice of technology and method of training would reflect the needs of the service to closely match the requirements of the individual worker. It might require close monitoring and, perhaps, customization of training, as well as significant worker buy-in to change. In selection of both technology and workforce, much effort might be needed because this kind of service requires high skill levels (as measured by years of education) and relatively high pays. Well-selected and implemented technology gives service workers a capability to customize the customer's various needs. This places computer graphic equipment implementation in Type I of Table 1.

Type II: Knowledge-embedded 'Goods-like' Services

When we contrast this with the typical implementation of automated technology in an automated car wash, we discover that many of the goals are the same - increased efficiency, repeatability, better conformance quality, etc. This is because the two are similar in that there is a significant product component in what is delivered: a drawing and a meal. However, the role of the person interacting with the technology is very different. In the above computer graphic example, the technology was an extension of the highly educated or experienced worker□□□enhancing their skills and building off of their knowledge. In the restaurant example, the situation is very different□□□the worker is now just an extension of the technology, and the technology has reduced or replaced the need for certain worker skills. As such, one could argue that the value-added is embedded in the technology, not the worker, and it is the technology that is enabled by the worker (by pushing the appropriate buttons when signaled, etc.). With technology, the workforce can standardize their work and service. This would be in Type II of Table 1.

Because of these differences, the implementation of technology in these knowledge- embedded environments would be managed differently too. As discussed above, while advanced technologies may have a prominent place in the product/process environment, in general, neither the nature of the service nor the nature of the production process is affected by the technology in a fundamental way. For example, worker

training in this environment would most likely be quite routine and standardized, and it is unlikely that the worker (car wash operator) would have significant input regarding the specific piece of equipment purchased. Additionally, there is less need to select a workforce with high skill levels and educational requirements. In such implementations, system-wide technology adoption/implementation strategies that can be learned from the experience of manufacturing sector might be useful.

Type III: Knowledge-based 'Pure' Services

Consider for example, the implementation of new communication technology now becoming popular in education that allows classes to be taught via satellite or Internet. Clearly, this is a knowledge-based service. The teacher/instructor/professor remains central to the process, and is providing the basis for the class. As such, worker (instructor) buy-in, training, and involvement in the process are keys to successful implementation. The new medium technology provides an extension of the instructors' capabilities, enabling him/her to reach students in locations that would not be possible through traditional methods. It is critical that the instructor knows the abilities and limitations of the technology in order to effectively use it. Often continuing learning/training might be needed. As in the case of computer graphic service, selection of appropriate technology for service might be critical. However, unlike our previous two examples, there is not a significant product component to this service. This significantly affects the technology implementation process. First, the goals of the technology are different from traditional production based improvements such as conformance quality and efficiency. The main benefit of this technology directly addresses the needs of a set of new customers who do not live in close proximity to the classroom. Rather than operating "behind the scenes" like in our computer graphic and automated car wash examples, in this case, the customer has significant interaction with the technology itself. In fact, the customer might have chosen to purchase the service (the class) on the basis of the offerings of the technology. The technology itself is designed to create attributes that the customer is aware of and finds desirable. Thus, implementing technology in such pure service environments, the customer himself would be more at the forefront in the selection process. Further, both the instructor (worker) and the student (customer) would need training in how to use the new technology. This differs from the above examples, where the customer might be oblivious to the technology itself.

Type IV: Knowledge-embedded 'Pure' Services

Our final illustration of the utility of the framework uses the example of package delivery (i.e., UPS, FedEx). Again, it is the technology that provides the main source of competitive advantage here. The mapping and order tracking technologies are the backbone of the elaborate delivery network. As in our example in the automated car wash, the worker in this environment (the driver and sorter) relies heavily on the technology to guide their daily activities. The worker responds to the technology's direction (i.e., creating routes), rather than the other way around. As such, technology implementation issues such as training and worker buy-in would resemble those in Type II, with customization and worker feedback playing a relatively limited role. The major focus of the adoption/implementation of new technology in this kind of service might be the way of system-wide competence enhancing in production process of service.

Unlike the automated car wash, however, firms operating such as package delivery operating in Type IV do not have a significant product component in their

service. As a pure service, the customer interacts with the process (and often the technologies - i.e., customer on- line tracking). As a result, the customer tends to play a greater role in the process as a whole. The customer interacts with the service provider to select the delivery options, and intangibles, such as driver courtesy, greatly affect customer satisfaction. As a knowledge-embedded service the "production system" can be standardized through new technology, but as a pure service the issue of interaction with customer might be a key factor in the technology implementation process and success.

Discussion And Implications

The widespread interest in the technology adoption/diffusion of the service sectors among academics and practitioners is a relatively recent phenomenon. This might reflect the fact that technology management in the service sector has significantly lagged behind that in the manufacturing sector. Service technologies have radically altered the strategic environment in ways that offer significant new opportunities and threats for service businesses [48, 51, 52, 53]. In addition, service technologies offer a variety of ways for service providers to add value within their own operations. Thus, the adoption of innovative technology in the service sector can have widespread impact on the value-added activities for a service firm or industry.

This paper proposes a classification scheme which, incorporating the idea of the source of the "value-added" and the degree of product component delivered, offers an effective method of classifying service for the management of technology. In view of the important relationship between customer value and service, this perspective focuses on how customer value is created, what mechanisms are utilized in "value-added", and how competence in service can be enhanced.

Each type of this classification scheme has important managerial and technological issues. In a service which has characteristics of significant product component and provides a customer value by service workforce (Type I), the adoption/implementation of new technology is aimed at enhancing effectiveness, improving existing skills and capabilities of the workforce, and does not eliminate the need for workers with knowledge and experience. The choice of technology and method of training would reflect the needs of the service to closely match the requirements of the individual worker. It might require close monitoring and, perhaps, customization of training, as well as significant worker buy-in to change.

As in the case of implementation of computer graphic equipment, new technology adoption in Type II (i.e., automated car wash, fast food) is aimed at increasing efficiency, improving quality, and reducing costs. As an example, Boston Chicken invested heavily in an information-management system. This system began at the point-of-sale (POS) terminals, which doubled as training aids. The system provided managers, staffers, and headquarters with instant communication with other parts of the network. In addition, the in-store computer system, Intellistore, helped store managers schedule labor, track inventory, and manage production. Intellistore also featured forecasting functions that help the manager estimate purchasing, staffing, and preparation requirements. However, in this kind of knowledge-embedded service, the workforce typically has a low skill level and is an extension of the technology. The technology has replaced the need for worker skills. Technology adoption/implementation is focused here on the competency enhancing abilities of the system, not on the capability of workforce. In this environment, technology implementation issues such as training and worker buy-in would be routine.

In a service which is knowledge-based and 'Pure' service component (Type III), the customer has significant interaction with the technology itself. The customer might have chosen to purchase the service on the basis of the offerings of the technology, and the customer himself would be more at the forefront in the selection process. In this environment, the technology would again be implemented differently. The new technology provides an extension of the service provider's capabilities, perhaps enabling him/her to reach more customers or provide unique product attributes that would not be possible through existing methods, as in the case of distance education. Because the worker is central to the value-added, worker buy-in, training, and involvement in the process are key to successful implementation. At the same time, traditional manufacturing goals such as quality improvement and cost reduction are not as common.

Like package delivery in our classification scheme, some services are both knowledge- embedded and 'Pure' service component (Type IV). Like our example in the automated car wash, the worker in this environment relies on the technology to guide their daily activities. In addition, technology implementation issues such as training and worker buy-in would resemble those in the case of automated car wash. However, in this environment, training customization and worker feedback play a relatively limited role. However, unlike Type II, as a pure service, the customer interacts with many of the service technologies and might be involved in the selection of technology, or at least its critical attributes.

The framework presented in this paper is designed to be a starting point upon which to build theory and establish effective management practice in each of the four types. The classification scheme as proposed provides essential managerial insights. It provides a richer framework in which to manage technology in services in that it incorporates two aspects of services (the source of core value-added and the degree of product component) critical to technology implementation. Therefore, it allows a better understanding of the nature of service within a technological context. As such, it incorporates the importance of technological innovation in service production, the factors underlying the process of customer value creation, and the means of enhancement of service production system, providing managers in technologically rich service industries a more comprehensive tool than currently available.

References

[1] Kandampully, J. (2002). Innovation as the core competency of a service organization: The role of technology, knowledge and networks, *European Journal of Innovation Management*, 5(1), pp. 18-26.

[2] Sirilli, G. & Evangelista, R. (1998). Technological innovation in services and manufacturing: Results from Italian surveys, *Research Policy*, 27, pp. 881-899.

[3] Quinn, J.B., Baruch, J.J. & Paquette, P.C. (1988). Exploiting the manufacturing-service interface, *Sloan Management Review*, 257(6), 45-56.

[4] Kellogg, D.L. & Nie, W. (1995). A framework for strategic service management, *Journal of Operations Management*, 13, pp. 323-337.

[5] Alic, J.A. (1994). Technology in the service industries, *International Journal of Technology Management*, 9(1), 1-14.

[6] Morone, J. & Berg, D. (1993). Management of technology in the service sector: Practices in the banking industry, *Journal of High Technology Management Research*, 4(1), 123-137.
[7] Hayes, R.M. & Thies, E.A. (1991). Management of technology in service firms, *Journal of Operations Management*, 10(3), 388-397.
[8] Vitale, R. (1986). The growing risks of information systems success, *MIS Quarterly*, 10(4), 327-334.
[9] Berg, S.V. (1973). Determinants of technological change in the service industries, *Technological Forecasting and Social Change*, 5, 407-426.
[10] Schooleman, S. (1993). Service, technology positions Pyxis for success, *Health Industry Today*, 56(6), 16-17.
[11] Empson, L. (2001). Introduction: Knowledge management in professional service firms, *Human Relations*, 54(7), 811-847.
[12] Behara, R.S. (2000). Process innovation in knowledge-intensive services. In: J.A. Fitzsimmons and H.J. Fitzsimmons (Eds.), *New Service Development*, Sage Publications, Inc., Thousand Oaks: CA.
[13] Fischer, M.J. (1996). Real-izing' the benefits of new technologies as a source of audit evidence: An interpretive field study, *Accounting, Organizations and Society*, 21(2, 3), 219-242.
[14] Thukral, I.S. (1995). Quality in Services through Design: An Integrated Approach, Unpublished doctorate dissertation, Rensselaer Polytechni Institute, New York.
[15] Lin, A. (1995). Far out: Distance education is more than a camera in a classroom, *Wall Street Journal*, Nov. 13, pp. R28+.
[16] Lee, M. (1995). Leading the way: College and campuses provide an insight into how technology may change the nature of instruction, *Wall Street Journal*, Nov. 13, pp. R28.
[17] Sasser, W.E., Olsen, R.P. & Wyckoff, D.D. (1978). *Management of Service Operations: Text, Cases, and Readings*, Allyn & Bacon, Massachusetts.
[18] Schmenner, R.W. (1986). How can service businesses survive and prosper?, *Sloan Management Review*, 27(3), 21-32.
[19] Hill, T.P. (1977). On goods and services, *Review of Income and Wealth*, 23, 315-318.
[20] Chase, R.B. (1981). The customer contact approach to services: Theoretical bases and practical extensions, *Operations Research*, 29(4), 698-706.
[21] Thomas, D.R.E. (1978). Strategy is different in service businesses, *Harvard Business Review*, 56(4), 158-165.
[22] Kotler, P. (1980). *Principles of Marketing*, Prentice-Hall, New Jersey.
[23] Lovelock, C.H. (1983). Classifying services to gain strategic marketing insights, *Journal of Marketing*, 47(3), 9-20.
[24] Hsieh, C. & Chu, T. (1992). Classification of service businesses from a utility creation, *The Service Industries Journal*, 12(4), 545-557.
[25] Quinn, J.B. (1992). *Intelligent Enterprise*, The Free Press, New York.
[26] Fitzsimmons, J.A. & Fitzsimmons, M.J. (1994). *Service Management for Competitive Advantage*, McGraw-Hill, New York.
[27] Shostack, G.L. (1977), Breaking free from product marketing, *Journal of Marketing*, 41(2), 73-80.
[28] Rathmell, J. (1974). *Marketing in the Service Sector*, Winthrop Publishers Inc., Massachusetts.
[29] Bateson, J. (1977). Do we need service marketing? In: P. Eiglier, E. Langeard, C.H. Lovelock.& J. Bateson (Eds.) *Marketing Services: New Insights*, Marketing Science Institute, Massachusetts.

[30] Zeithaml, V.A., Parasuraman, A. & Berry, L.L. (1985). Problems and strategies in service marketing, *Journal of Marketing*, 49(2), 33-46.
[31] Edgett, S. & Parkinson, S. (1993). Marketing for service industries: A review, *The Service Industries Journal*, 13(3), 19-39.
[32] Verma, R. & Boyer, K.K. (2000). Service classification and management *Journal of Business Strategies*, 17(1), 5-24.
[33] Cook, D.P., Goh, C., & Chung, C.H. (1999). Service typologies: A state of the art survey, *Production and Operations Management*, 8(3), 318-338.
[34] Lovelock, C.H. (1991). *Services Marketing*, Prentice Hall, New Jersey.
[35] Lovelock, C. H. & Yip, G. S. (1996). Developing global strategies for service business, *California Management Review*, 38(2), 64-86.
[36] Collier, D.A. (1985). *Service Management: The Automation of Services*, Reston Publishing Company, Virginia.
[37] Collier, D.A. (1983). The service sector revolution: The automation of services, *Long Range Planning*, 16(6),10-20.
[38] Perrow, C. (1967). A framework for the comparative analysis of organizations, *American Sociological Review*, 32, 196-208.
[39] Thompson, J.D. (1967). *Organizations in Action*, Basic, New York.
[40] Dubin, R. (1968). *Human Relations and Administration* (3rd edition), Prentice Hall, New Jersey.
[41] Mills, P.K. & Moberg, D.J. (1982). Perspectives on the technology of service operations, *Academy of Management Journal*, 7(3), 467-478.
[42] Barras, R. (1986). Towards a theory of innovation in services, *Research Policy,* 15(4), 161-173.
[43] Mills, P.K. & Margulies, N. (1980). Toward a core typology of service organizations, *Academy of Management Review*, 5(2), 255-265.
[44] Harvey, J., Lefebvre, L.A. & Lefebvre, E. (1997). Flexibility and technology in services: A conceptual model, *International Journal of Operations & Production Management*, 17(1), 29-45.
[45] Lewis, M.A. (2002). Selecting and implanting service technology: Control, uncertainty and competitive advantage, *The Service Industries Journal*, 22(2), 17-42.
[46] Clemons, E. (1986). Information systems for sustainable competitive advantage, *Information and Management*, 11(3), 131-136.
[47] Feeny, D. and Ives, B. (1990). In search of sustainability: Reaping long term advantage from investment in information technology, *Journal of Management Information Systems*, 7, 27-46.
[48] Guile, B.R. & Quinn, J.B. (1988). *Technology in Services: Policies for Growth, Trade, and Employment*, National Academy Press, Washington, D.C.
[49] Davis, J.E. (1996). Citibank ambushed by ATM networks, Fortune, May 13, pp. 34.
[50] Chase, R.B. (1978). Where does the customer fit in a service operation?, *Harvard Business Review*, 56(6), 137-142.
[51] Quinn, J.B. & Paquette, P.C. (1990). Technology in services: Creating organizational revolutions, *Sloan Management Review*, 31(2), 67-78.
[52] Quinn, J.B., Baruch, J.J. & Paquette, P.C. (1987). Technology in services, *Scientific American,* 257(6), 50-58.
[53] Skinner, W. & Chakrabarty, K. (1982). *The Impact of New Technology: Challenges, People and Organizations in Service Industries*, Pergamon Press, New York.

Use Case Modelling of Bingham University Library Management System

[1]Faki A.S, [2]Ogedebe P.M.

[1,2] Department of Computer Science, Faculty of Science and Technology,
Bingham University, Karu - Nasarawa State, Nigeria
faki.silas@binghamuni.edu.ng. peter@binghamuni.edu.ng

Abstract

With the advent of object oriented design, universal markup language (UML) has become prominent in software industry. Software is better modeled with the use of UML diagrams like use cases which provide a better flow of logic and comprehensive summary of the whole software system in a single illustration. In this paper, we are able to model a University library which shows clear flow of logic and hence easy easy for coding.

Keywords: *Actor, Use Case, UML, Login*

Introduction

The principal medium for capturing requirements in the Unified Process is the use-case diagram. Use-case diagrams illustrate the relationship between a software system and its users. They also describe how each type of user will interface with the system. In this paper, we illustrated use case by modeling a University Library Information System. The use of use case made the coding aspect of the software easier and also shows a clear flow of logic in the system. The rest of the paper is presented as follows: II Review of related literature, III Shows the Library Information System design using use case, IV Present entity diagram from the use case and V The summary of work.

Review of Related Work

As object-oriented software engineering gains prominence in software practices, use cases have enjoyed a seemingly explosive growth to become ubiquitous in both development methods and development practice. Part of this ubiquity can be attributed to their utility; use cases have proved to be versatile conceptual tools for many facets of design and software development.

A use case defines a sequence of actions a system performs that yields an observable result of value to a particular actor. In other words, a use case describes a primarily functional and also non-functional requirement from the perspective of an actor achieving particular goals. The goal of object oriented use case analysis and design according to [1] is to transform the 'black box' use case specification into a 'white box' use case realization.

As an effective bridge between usability engineering and user interface design on the one hand and software design and development on the other, part of the promise that use cases offer is due precisely to their chameleon-like adaptability [2]. For requirements engineering, use cases provide a concise medium for modeling user requirements; in the hands of user interface designers, use cases can become a powerful task model for understanding user needs and guiding user interface design; for software engineers, use cases guide the design of

communicating objects to satisfy functional requirements.

As observed by [2], most commonly used, use cases describe the actual interaction between external users (or system actors) and a system through a particular interface. Because they are expressed in concrete terms, such use cases are best referred to as concrete use cases. Also an essential use case can be looked upon as a single, discrete, complete, meaningful, and well-defined task of interest to an external user in some specific role or roles in relationship to a system, comprising the user intentions and system responsibilities in the course of accomplishing that task, described in abstract, technology-free, implementation independent terms using the language of the application domain and of external users in role.

[3] differentiate use case and use case scenarios by defining the first with three keys things, (i) the actor or actors involved (ii) the system being used (iii) the functional goal that the actor achieve using the system. Use case scenario is seen as different outcomes based on circumstances.

[4] describe use case as a technique for capturing and communicating functional requirements for software development. Use cases are written from the perspective of the user as a flow of events. The user is called an "actor" and the narrative of the flow of events between this actor and the system is called the "use case." Use cases are literally the specific "cases" for which the actor wants to "use" the system. Use cases differ from declarative statements in two primary ways. They describe functional requirements from the user perspective rather than the system perspective, and they provide a coherent goal focused flow of events rather than a set of discrete declarative statements. A fully described use case will have a main or basic flow as well as alternate flows [5]. The alternate flows describe regular variants to the main flow as well as error handling or unusual situations.

Library Management Design Using Use Case

To model software using object oriented design, a case study of Bingham University Library Management System is used. Software is developed to automate the Bingham University manual Library. The system will be stand alone and will be designed with the following functionalities:

Issues of Books

A student of any course should be able to get a book issued.

Books from general section are issued to all but departmental books are strictly issued to students in the departments.

A limitation is imposed on the number of books a student can borrow.

A maximum of 2 books from departmental and 3 from general section can be borrowed by a student for 15 days.

Software takes in the current system date as the date of issue and calculates the date of return. A bar code detector is used to save the student as well as the book information.

The due date for return of the book is stamped on the book.

Returning of Books borrowed by Students.

Any person can return a borrowed book. The student information is displayed using the bar code detector. The system displays the student's details on whose name the book(s) were issued as well as the issued and return date. The system operator verifies the duration for the borrowed book. The information is saved and the database updated.

Query Process

The system is able to provide the following information.

- Availability of a particular book
- Availability of a book of any particular author

- Number of copies available of a particular book.
- Generate report of available books in the library

Use Cases

Use case diagrams is a simplest representation of a user's interaction with the system and also depict the different types of users of a system and the various ways that they interact with the system. From the problem definitions, we can identify four majors' actors (Librarian, Operator, Bar Code Reader (BCR) and User) within the system. Their use case is given in Figure 1.

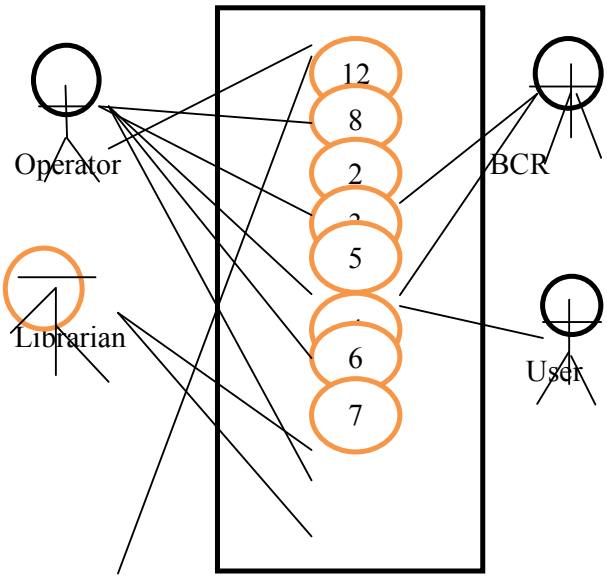


Figure 1: Use case diagram for Bingham University Library Management System.

Objects name in the use case are, 1: Login, 2: Issue Book, 3: Return Book, 4: Query Book, 5: Maintain catalogue 6: Generate report 7: Maintain Login 8: Maintain Student details.

Use Case Description

The description of the use cases are given as follows:

Login

These use case introduces the procedure for logging in to the University Library management System based on user privilege.

Here, the operator takes care of the following: issue books, return books, Query books, maintain catalogue, and maintain student details.

Also the Librarian maintain login and generate report.

Actors

Operator and Librarian

Pre-Condition

None

Post-Condition

If use case is successful, the user logged into the system, otherwise the system state is unchanged.

Logic Flow

Basic Flow

This use case starts when the use wishes to log into the University Library Management System. The following action can be trigger.

- The system request the user to enter his/her user_id and password.
- The actor enter user_id and password
- The system validates the user_id and password and check for his/her privileges.
- If the user is an operator, the system present operators menu.
- Otherwise, if the user is Librarian, the system present Librarian menu.
- The use case end.

Alternate Flow

Invalid name/Password

If the system received an invalid user_id or password, an error massage is displayed and the use case ends.

Special Requirement

None

Related Use Case

None

2. Issue Book

This use case documents the procedure of issuing a book for following accounts.

- General (15 days)
- Departmental Book (for the semester)

Actors

Operator, Barcode Reader

Pre-Condition

Operator must be logged in to the system

Post-Condition

If use case is successful, the book is issued to the student in his/her general or departmental account, otherwise the system state is unchanged.

Logic Flow

The use case starts when a student wants to get a book issued.

- The system reads and validates the student's information using the Bar Code reader.
- The System reads the book information using the Bar Code Reader.
- The return date of the book is calculated as per the account in which the student wishes to get the book issued.
- The book and student information is saved in the database.
- The issued details are sent to the printer to generate the receipt.
- The use case ends.

Alternate Flow

Unauthorized student

If the system does not validate the student, an error message is flagged and the use case ends.

Book Accounts if Full

If the student has already borrowed the required number of books, the request for issue is denied and the use case ends.

Course Mismatch

If a student requests book from a departmental library that is not his/her department, the request is denied unless under special cases and the use case ends.

Special Requirement

None

Related Use Case

Generate Barcode

Return Book

This use case documents the procedure of returning a book and calculating the fine amount if the student has returned the book after the specified return date.

Actors

Pre-Condition

The operator must be logged into the system.

Post-condition
If use case is successful, the book is returned to the library and if needed, a fine is calculated, otherwise the system state is unchanged.

Logic Flow
Basic Flow
This use case starts when a student wants to return a book.

- The system reads the book's information using Bar Code Reader.
- The book is return to the library
- The student and book database is updated
- The returned details are sent to the printer to generate receipt
- The use case ends.

Alternate Flow
Late return of book
If the book is returned after due date, fine is calculated and database is updated accordingly. The use case ends.

Special Requirement
None

Related Use Case
Generate Barcode

Query Book
This use case documents the procedure for searching a book based on the specified criteria, which are:

- Search by Author Name
- Search by Title Name

Actors
Operator, user

Precondition
Operator user must be logged into the system.

Post-Condition
If use case is successful, the book details are displayed.

Logic Flow
Basic Flow
This use case starts when a student wants to search for a particular book.

- The system displays the various search criteria to the user.
- The user selects the search criteria
- The result is displayed to the user
- The use case ends.

Special Requirement
None

Related Use Case
None

Maintain Catalog
This use case documents the procedure for updating the catalog of the library.

Actors
Operator

Pre-Condition
Operator must log into the system

Post-Condition
If use case is successful, the book should be updated, otherwise the system state is unchanged.

Logic flow
Basic Flow
This use case starts when the operator wishes to add, delete or modify some details in the library.

- The corresponding changes are saved in the database
- The use case ends

Alternate Flow
None

Related Use case
None

General Reports

This use case documents the procedures for generating reports as desired by the Liberian

Actors
Librarian

Pre-Condition
Librarian must be logged into the system

Post-Condition
If use case is successful, the various reports, regarding the details of books available in the library at any given time are generated.

Logic Flow
Basic Flow
This use case starts when a Librarian wants to generate reports of the books available in the library.

- The system displayed the various reports generating criteria to the user, which can be the books issued to students at a particular time, books available in the library etc.
- The Librarian selects the criteria and enters the various parameters based on the criteria selected.
- The system generates the report and sends it to printer for printing.
- The use case ends.

Alternate Flow
Printer out of Paper or low ink
If the printer goes out of paper or low ink, then the printing operation is aborted and the necessary action needs to be taken, which can be feeding paper to the printer or replacing think cartridge. The use case ends.

Special Requirement
None

Related Use Case
None

Maintain Login

This use case documents the procedure for maintaining log in details

Actors
Librarian

Pre-Condition
Librarian must be logged into the system.

Post-Condition
If use case is successful, the login details should be updated, otherwise the system state is unchanged
.
Logic Flow
Basic Flow
This use case starts when the Liberian wishes to add, delete or modify some details of login.

- The corresponding changes will be done
- The use case ends.

Alternate Flow
None

Special Requirement
None

Maintain Student Details
This use case documents the procedure for maintaining student's details.

Actors
Operator
Pre-Condition
Operator must log in the system
Post-Condition
If use case is successful, the student details should be updated, otherwise the system state is unchanged.

Logic Flow
Basic Flow
This use case starts when the operator wishes to add, delete or modify some details of students.

- The corresponding changes will be done

- The use case ends.

Alternate Flow
None
Special Requirement
None
Related Use Case
.
None
Class Diagram of the Entity Class
From the use case description, we can have a class diagram as the one given in figure 2 .These entity classes generally becomes tables in the database

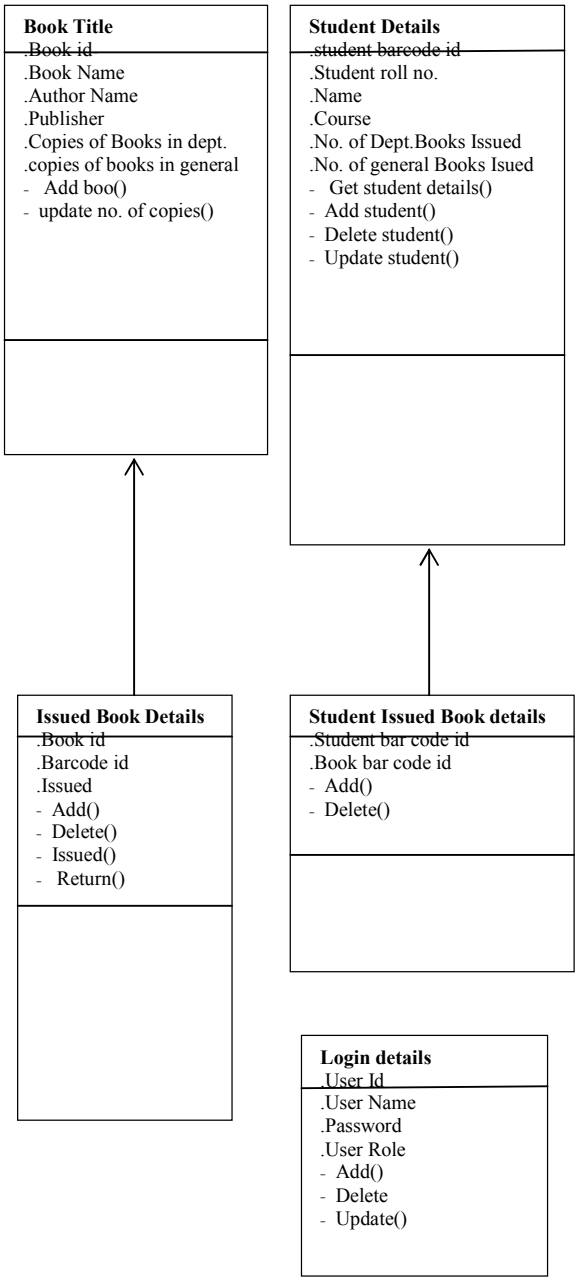


Figure 2: Class diagram for Bingham University Library Information System.

Summary

In summary, a well-prepared use case is worth its effort. Once the client has agreed to the use cases, the project managers can plan their schedule, and the developers can then have a clear understanding of what they must develop. From personal experience, we make bold to state that, while a use case is very beneficial, they are rarely perfect, but they always serve a useful purpose.

References

[1] Peter H (2004), Use case-based Software development. Retrieved from, http://haumer.net [Accessed on 18/04/20012].

[2] Larry L.C, Lucy A.D. (2002), Structure and Styles for Use Cases for User Interface Design. Constantine and Lockwood Ltd.

[3] Jarson G. (2006), Retrieved from, www.parlezuml.com [Accessed 18/04/2014].

[4] Dennise. E. (2005), Use Case: Background, Best Practices and Benefits. MKS White Paper in Application Engineering.

[5] Aggarwal.K.K, Yogesh S. (2008), Software Engeneering. Third Edition. New Age International (P) Limited Publoishers, New Delhi.

Investigating the Benefits of Information and Communication Technologies (ICTs) on Practices of Enterprises: The Nigerian Perspective

[1]Oladimeji, S. A., [2]Babatunde B. Olofin, and [3]Rasheed A. Raji,

[1,2]Department of Computer Science, Federal Polytechnic Nekede, P O Box 4545, Enugu, Nigeria
[3]Department of Computer Science, Federal Polytechnic Damaturu, P O Box 358, Damaturu, Nigeria
[1]Cell: +2347030623266; Email: dimejibiodun@hotmail.com. [2]*Cell: +2348033215972; Email: bbolofin@gmail.com*
[3]*Cell: +2348061596436; Email: rajiayanda@gmail.com*

Abstract

Information and Communication Technologies (ICT) are widely used by organizations to enhance enterprise competitiveness. This study provides an overview of the current state of affairs of the ICT adoption in SMEs in private and public organizations in Nigeria. It investigates ICT infrastructure, productivity and business application software used, drivers for ICT investment, perceptions about business benefits of ICT, outsourcing trends and availability of help and advice on ICT adoption. The study has also investigated major barriers in ICT adoption and the findings of the study are consistent with other similar studies. The study identified the need for more training facilities for adopting ICT in SMEs. Additionally, the study identified that there is a need for the Government to provide guidance on suitable ICT products and services at an affordable cost as well as provide incentives to promote ICT investment and usage e.g. soft loans, availability of professional advice and consulting at no/low cost to SMEs. This is the first study on the status of ICT adoption and usage by SMEs in Nigeria. The findings of this research will provide a foundation for future research and will help policy makers in designing policies to further enhancing usage and ICT adoption in SMEs in Nigeria resulting improved productivity and competiveness.

KEYWORDS: Information and Communication Technology (ICT), Nigeria Enterprise Practices, Business Management.

Introduction

Information and Communication Technologies (ICT) have an important impact on businesses in developed and developing countries. ICT is creating new opportunities by enabling design and delivery of digital goods, allowing firms to increase margin and revenue by accessing foreign markets directly. Papaioannou [1] explored the effects of ICT on productivity and economic growth in both developing and developed countries and concluded that ICT has a positive and meaningful effect on productivity and economic growth. VanDijk [2] indicated that ICT is being seen as an agent of economic development in South-East Asian countries especially in South Korea. Burke [3] observed several important benefits from owning websites, such as having new customers and additional sales by firms. Certain infrastructure must be in place in order to benefit from ICT adoption so as to deliver better services and explore new

business opportunities. According to Limi [4] infrastructure is one of the most important driving forces for economic development. Measuring ICT at the firm level could help countries improve the production and quality of their ICT for development. The analysis of data on measuring the impact of ICT on enterprise practice aims at providing organization policymakers with better tools to design, monitor, and evaluate their ICT strategies. Aside from infrastructure, other factors that help ICT success are availability of skilled ICT personnels and budget to invest in ICT [4]. ICT is one of the key ingredients to enhance a company's competitiveness. ICT platforms (such as PCs, mobiles, internet, etc.) have four main contributions to organizations. First, they give more visibility to business enterprises. Second, they provide more information to small firms. Third, they allow enterprises to overcome traditional trade barriers. Finally, they facilitate financial transactions [5]. ICTs make services more easily tradable and increase productivity in manufacturing enterprises. Furthermore, the use of e-mail, e-commerce, and social media network have significantly cut down on the physical transportation involved in sending mail, banking, advertising, and buying goods. Clift [6] notes that the private sector should not only be able to invest in an ICT infrastructure but also use ICTs as a means of competitive advantage to conduct business in the form of commercially-driven connectivity, software, technology, e-commerce, online transactions and so on. Based on the above studies, there is little doubt about the benefits of the ICT as a tool to access the global market. Still, underdeveloped countries have their own challenges in adopting ICT and reaping the benefits that developed countries have gained through ICT.

Little research is currently available that discusses ICT status of ICT adoption and usage in organizations in the Middle East in general, and Gulf Cooperation Council (GCC) countries, in particular. The purpose of this paper is to fill in this gap by investigating the current state of ICT adoption in Nigerian enterprises. The term ICT in this research refers to a wide range of information and communication technologies, including IT infrastructure, wired or wireless networks, business productivity software, enterprise software, and data storage. The aim of this research is to investigate the current state of ICT adoption in Nigerian enterprises. The outcome of the study would be of particular interest to private and public enterprises who would like to enhance their use of ICT in Nigeria. The findings will also have implications for other West African countries as they seek efficient and effective ways to improve their ICT. The sections covered in this paper includes: 1) – The Literature Review; 2) – The Research Methodology; 3) – The Research Findings & Results; 4) - Conclusions of the paper with Limitations and Suggestions for future research.

Literature Review

Evidence in research literature suggests that ICTs can contribute significantly to the efficiency, productivity and innovation of a firm. The use of ICT enables the production of goods in a shorter amount of time with the assistance of computerized systems. Studies also show that investments in ICT had a considerable effect on the productivity of the labor force and on economic growth [7]. Previous research also finds that, in addition to computer presence, Internet use and web presence are also reflected in higher labor productivity. ICT has influenced almost every aspect of an organization's activities from customer prospect to post-sales services [8]. However, earlier studies have noted that African countries are still falling behind developed

countries in terms of both use and spending on ICT [9, 10]. One study found that while many governments in the African continent have embarked on projects to drive growth through IT transformation, many governments still lacked all elements necessary to make these projects a success [11].

ICT sector is one of the foremost sectors in Europe and affects economic growth across the economy in many ways. For instance, the ICT sector share of total business value added is 8.5% and the ICT segment employment constitutes 3% of total business sector employment in the EU [12]. Furthermore, ICT investments help to raise labor productivity and the most important benefits of ICT arise from its effective use. ICT is a tool that will only work in enterprises that are structured to use it and that require change. In the USA, the ICT revolution has stimulated enterprise re-organization and has altered the terms of competition. US businesses have become more adept at getting value from their ICT activities. Thus ICT spending in the US has jumped to 5.4 % in 2010 [13].

In the USA, Europe, and Australia, a high percentage of firms have access to the Internet, thereby giving them an access advantage to the global markets. In Asia, Japan, Korea, and China are leading in this regard, and recent ICT product and services have accelerated and expanded their access to world markets [14]. The World Bank [15] emphasized that governments can create competitive markets that grow faster, cost less, facilitate innovation, and respond better to user needs if they would open their telecommunications markets through well-designed reforms resulting in increased private investment and ICT development. For example, Roeller & Wavermant [16] showed that between 1970 and 1990, one-third of Germany's economic growth was attributed to an increase in the penetration rate of fixed telephone lines. Hamilton [17] argued that investment in basic telecommunications in Africa had a positive impact on economic, political and institutional development. A number of scholars hafve also validated the view that ICTs such as the internet can even inspire speedy democratization in regions of the world such as the Middle East [18]. This has been seen recently through events such as the "Arab Spring" witnessed in Egypt, Libya, Syria, Tunisia, Yemen and other Middle Eastern countries.

ICT Adoption in Developing Countries with Special Reference to the Middle East and GCC countries

ICT can be used as a strategic lever for socioeconomic development and as a competitive tool in an increasingly global and deregulated market [19]. Shih et al. [20] have found that for developing countries to realize potential benefits of IT, policymakers should look for ways to promote IT investment as well as developing investment resources, complementary assets, and openness to external influence. ICT privatization in developing countries has been viewed by many scholars as the key method for modernization and expansion of public telecommunications networks [21, 22, 23, 24]. Privatization of telecommunication infrastructure and ICT in general, has also helped to boost foreign direct investment (FDI), a major source of ICT financing. Heeks [25] found that ICT project failures in developing countries is higher than developed countries, possibly due to lack of technical and human infrastructure. Bodla and Rashid [26] identified that lack of infrastructure, low per capita income, unskilled human capital, political and economic structure and conservative bureaucratic approach were the main barriers in adoption of ICT in developing countries. Mofleh et al. [27] have found that major ICT initiatives in developing countries have failed in achieving major development

outputs. Particularly, SMEs in developing countries have been slow in adoption and diffusion of ICT. Kapurubandara [28] classified various factors contributing to the slow adoption of ICT in SMEs in developing countries into Internal and External Barriers.

In the late 1990's, Middle Eastern governments invested heavily in ICT, enabling them to not only renew, but expand their ICT infrastructures by implementing new technologies. From 1995 to 2002, ICT spending on equipment, software and telecom services in the Middle East increased sharply. GCC enterprises still face key challenges as they strive to increase ICT adoption and effectiveness. For instance, in human lack of information about suitable ICT solutions and implementation were some of the major barriers in adopting ICT [29]. Booz Allen [30] has identified lack of key enabling resources, inadequate infrastructure, transient funding and oversight as the main barriers in ICT adoption in GCC countries.

Privatization of telecommunications in the Middle East and the role of telecommunications provider in the expansion of ICTs, started in the early 1980's with the establishment of Kuwait's Mobile Telecom Company (MTC). Between 2000 and 2008, the percentage of firms with access to the Internet has increased substantially across all GCC countries. The highest rate of uptake of Internet in the ranking of GCC countries was in UAE followed by Saudi Arabia, Kuwait and Qatar. According to El-Shenawy [11], Arab ICT indicators are still not sufficient, not available and not publicized. Abdallah and Al-badri [31] examined the literature on ICT in the Arab world in order to glean the level of ICT investment and acceptance, and to attempt to understand the interplay of cultural practices and values on the successful implementation of ICT initiatives. Hamade [32] has categorized major reasons for ICT adoption in Arab countries into two categories: one related to the basic infrastructure and the other related to government's policies and regulations. ICT has played a major role in the Middle East recently, with the Internet being central in driving the political upheavals and revolutions witnessed in the region since the beginning of this year. Social networks have been essential in this process, allowing people to connect and mobilize [33].

ICT Adoption in Nigeria

The establishment of the National Information Technology Development Agency (NITDA) in 2001 was one of the first high-level policy initiatives to improve and promote ICT for development in Nigeria. This governmental agency leads Nigerian's implementation of ICT initiatives to help ensure a balanced investment in technology, research, and development leading to the development of new products and processes that spur productivity and efficient operations. One of the identified agents through which the world will constantly experience change is technology. In the business of trying to make information available in the right form to the right user both at the personal and organizational levels, and at the right time, the bid to cope with great flood of information has led to the need for a more sophisticated way of handling information faster and better. According to Anyakoha [34], information technology is "the use of man-made tools for the collection, generation, communication, recording, re-management and exploitation of information. It includes those applications and commodities, by which information is transferred, recorded, edited, stored, manipulated or disseminated". Hawkridge [35] describes information technology as a revolution which has penetrated almost all fields of human activity, thus transforming economic and social life. UNDP [36] asserts that even if

sustainable economic growth facilitates the creation and diffusion of useful innovations, technology is not only the result of growth but can be used to support growth and development. ICTs are credited with the ability to transform, and deep and significant changes are expected from their widespread use in Africa. From this stand point Africans can take maximum advantage of the new technologies even if major challenges remain. These challenges include adapting ICTs to local conditions and uses in developing countries, and allowing each country understand those innovations and adjust them to their own development needs.

Therefore, development in Nigeria depends on the country's capacity to create wealth to significantly reduce poverty and to raise its capacity to create wealth at a sustainable level. In June 1996, the United Nations Commission on Science and Technology Development (UNCSTD) in collaboration with IDRC proposed five development indicators that focused on the improvement of the quality of life: education, health, income, governance, and technology [37]. If we consider these five as key indicators of development for Nigeria, ICTs can be socially beneficial only if they contribute to poverty eradication (higher income), improved health and education, better use and more equitable sharing of resources, and raising participation in the decision-making processes (and in this regard, access to information is crucial).

ICTs have been the basis for human existence from time immemorial and this has driven man to continuously seek ways to improve the processing of information and communicating such information to one another irrespective of distance and on a real-time basis [38]. Surviving in the information age depends on access to national and global information networks. ICTs are the bedrock for the survival and development of any nation in a rapidly changing global environment, and it challenges us to devise initiatives to address a host of issues such as reliable infrastructure, skilled human resources, open government, and other essential issues of capacity building [39]. At the heart of technology lie two main or branches of technology: computing and telecommunication. The technologies covered are the computer system, Internet/electronic mail (e-mail), mobile phone, and fax machine.

Research Methodology

The data for this study was collected through a survey questionnaire sent to random companies in which an IT division was listed in the company structure. The questionnaire was based on a similar study undertaken in Libya by [29]. The reason for adopting the same questionnaire was to facilitate comparisons between the status of ICT adoption and practices in the two African countries. The questionnaire survey approach was used for its various benefits: such as to detect relationships that are common across the organizations [4], exhibit considerable precision in collecting and reporting data [41], an inexpensive approach for collecting data [41], and offering anonymity [42, 43]. The questionnaire was structured to obtain data on current usage and adoption of ICT in organizations. It was designed to be answered by a Senior Manager or Head/In charge of the IT (Information Technology) department of the company that participated. The survey consisted of 25 questions which included the current ICT status and ICT use in the company, and the impact of ICT investment on cost reduction, efficiency, performance and effectiveness. A pilot study was first conducted with five companies. Based on their feedback, changes were made to the layout of the questionnaire, with a view to improve readability and to reduce the amount of time to answer the survey.

Survey Questionnaire was mailed, and

in some cases personally delivered, to 157 IT managers or Heads of IT departments of public and private organizations in Lagos, Abuja & Port-Harcourt. 102 usable questionnaires were returned from the companies who have adopted ICT and responded to our survey achieving an overall response rate of over 65%. For the purpose of this research we adopted the following definition of SMEs: businesses with up to 50 employees were classified as Small enterprises, between 50 and 100 employees as Medium enterprises, and more than 100 employees as Large enterprises.

RESULTS

Organization Types

Of the 102 respondents, 26% were classified as Small enterprises and 16% as Medium-size enterprises, and 58% as large enterprises. ICT infrastructure, Internet connection type, IT staff, usage of enterprise software, and type of website were used as a measure for ICT usage.

ICT Infrastructure

Table 1 shows that desktop, laptop, or handheld computers were used by 93% of the surveyed companies. The reason being is that our sample was based on only those companies who adopted some form of ICT in their business (e.g. Computers). This result was not very surprising, as in the UK, 30% of micro businesses do not use computers at all [44]. Business productivity software such as Microsoft Word, Excel and PowerPoint were used by 82% of the surveyed firms. Also, network and data storage solutions were used by the majority of organizations surveyed

Table 1: IT Solutions Used within Organizations

Rank	ICT Usage	Percentage
1	Computers	93%
2	Productivity Software	82%
3	Wired Networking	74%
4	Wireless Networking	66%
5	Data Storage Solution	65%
6	Network Security Solution	64%
7	Enterprise Software	53%
8	Other Solution	12%

Internet Connection Type

The type of internet connection in organizations largely indicated the required bandwidth. Overall, 92% of the sample companies in our survey used Internet. 6% of the respondents used high speed broadband (ISDN, ADSL, DSL), 65% used very high speed broadband (T1, ATM, frame Relay, etc.), 23% use satellite and 6% either had no internet connection or did not respond. This was consistent with other studies. In a recent survey of SMEs in the UK, 78% of SMEs use Internet in their business [45] while the number of users in Nigeria was more than 92% based on our survey.

IT Staff

Unlike the commonly held belief that SMEs often lack skilled IT staff, 70% of the firms in Nigeria had IT/IS departments with full-time IT staff and only 28% of the surveyed firms did not have full-time IT staff. The remaining 2% did not respond to the question. This may be because 58% of the survey respondents belong to large organizations and 16% to medium organizations and thus could afford to have full-time staff as compared to small organizations (26%).

Usage of Enterprise Software

In our survey, 83% of respondents used Finance and accounting software, 63% used Human Resource Management (HRM) software, and 48% inventory management. One-third used Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) (Table 2). The result seemed to be similar to Software.

[29] that indicated 84% of the surveyed SME firms in Oman used finance and accounting enterprise software. It seems that the level of usage of CRM, ERP, Supply Chain Management (SCM) and E-commerce is quite low with most of the organizations using Finance or Acounting and HRM .

.

Table 2: Usage of Enterprise Software in the Organization

Rank	Software	Percentage
1	Finance/Accounting	83%
2	Human Resource Management	63%
3	Inventory Management	48%
4	Customer Relationship Management	38%
5	Enterprise Resource Planning	34%
6	Supply Chain Management	23%
7	E-commerce	19%
8	Others	16%

Types of Website Used

Unlike businesses in developed countries, the sample companies in Nigeria have not managed to utilize and use commercial websites for online sales. Results shows that less than 1% of the firms had dynamic commercial websites which helped them reach new customers and conduct e-business. As for informational websites, 53% of the surveyed enterprises ran websites which simply introduced the business and published their contact information. About 19% of the businesses had no website, the main reason being the lack of internal technical staff and high maintenance costs over the long term. This indicates that companies are not fully utilizing the Internet for buying and/or selling goods or services. One of the reasons may be that the level of exposure of the populace to the services of Internet is still at the lowest ebb. Moreover, people can physically visit organizations easily to buy products and/or services and do not need to order online. Another reason might be that organizations are focusing on the local market and have not expanded their business to other countries.

Investments in ICT

IT Budget & ICT Investment Drivers

Twenty-two per cent (22%) of the sample companies assign less than 10% of their annual budget to ICT investment while 39% of the firms invest between 10% and 20%. Furthermore, 25% invest between 20% and 40%, and 14% of the surveyed firms assign greater than 40% of their budgets to ICT. This shows that Nigerian companies realize the importance of IT, and are spending a significant amount of their budget on ICT. The main driving forces for ICT investment were to provide better and faster customer service (65%), and to

stay ahead of competition (69%).

Number of Competitors

A healthy competition drives organizations to be more competitive. Only 4% of the enterprises had more than 20 direct competitors. About 15% of Nigerian companies had 10-19 competitors, 26% between 5-9 competitors and 15% between 1-4 competitors. This shows that there is relatively low competition among companies in Nigeria, whereas in Libya, 50% of the enterprises had more than twenty direct competitors [29].

Competitive Strategy

One way of competing is to differentiate one's business from the competition. The surveyed companies have chosen the approach of providing the highest quality products and services (40%) to their customers as the principal method for differentiating, as well as establishing, long-term relationships with customers (25%) as illustrated in Figure 1. It seems that a majority of organizations do not have a well- defined strategy for ICT use and adoption. Perhaps they have implemented ICT because their competitors are using it in their respective businesses.

Figure 1: Firms' Approach to Differentiate Business from its Competitors

Barriers to ICT Investment

With regard to barriers to ICT investment, 46% firms felt that a lack of necessary internal skills was a major barrier. Lack of availability of relevant information and advice on suitable and effective technologies was also one of the major barriers. One-third of the respondents felt that the costs of implementation are too high. Other barriers included businesses having no time to implement ICT projects, lack of top management support, bad experiences in the past, and government regulations and requirements (Table 3). These findings are consistent with other studies [45, 29]. These results further emphasize the need for more training facilities in ICT for Nigerian businesses, measures to provide ICT products and services at an affordable cost, and availability of free professional advice and/or consulting services at a reasonable cost to the businesses.

These findings are consistent with [29].

As mentioned earlier, the Nigerian government created NITDA in 2001 to assist governmental, educational, and private institutions in becoming technologically connected. However, a number of organizations felt that the monetary costs of ICT solutions and implementation were too high.

Table 3. Barriers to ICT Investment

Rank	Barriers to Investment	Percentage
1	Lack of Necessary Internal Skills	46%
2	Lack of Time to Implement ICT Project	35%
3	Monetary Cost	30%
4	Lack of availability of Information	24%
5	Government Regulation	21%
6	Lack of top Management support	20%
7	Bad experience in the past	19%
8	Uncertain about retain	12%

Realization of Business Performance Improvements

Table 4 shows that those companies who have adopted ICT have realized that ICT has increased better relationships with their customers and suppliers, increased revenue, and helped in cutting costs. These organizations are very positive in continuing to invest and harvest those benefits in the future.

Table 4: Benefits due to ICT Adoption

Rank	Benefits due to ICT Adoption	Respondent %
1	ICT will increase better relationship	90
2	ICT has increased better relationship	82
3	ICT will reach new customer	81
4	ICT will increase revenue growth	80
5	ICT will expect cut in cost	78
6	ICT has increased revenue growth	66
7	ICT has cut cost	62
8	ICT helped beyond area	53

ICT Implementation and Outsourcing

Figure 2 shows that, overall, 89% of organizations outsource some portion of their ICT functions. Figure 2 also shows that 27% of Nigeria businesses outsourced more than 50% of their activities, 32% outsourced 25% to 50% of their activities, 15% outsourced between 10% and 25% of their activities and 15% outsourced less than 10% of their ICT activities. It seems to contradict with the earlier result in which 70% of organizations had an IT department, possibly indicating that they may not have all the capabilities they need thus the need to outsource. A study by Harindranath et al. [45] found that 50% of the firms in their survey used external consultants for ICT matters
.

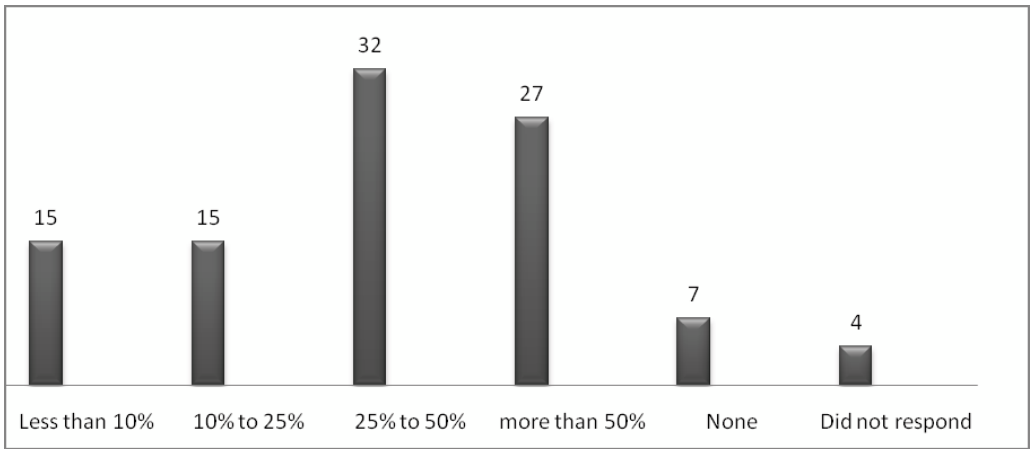


Figure 2: ICT Outsourced Percentage

Resources Used for ICT Implementation

While it is important to understand which ICTs were adopted and used within Nigerian companies, it is also important to understand which internal or external resources were used to implement these technologies. Most of the enterprises surveyed used internal resources to implement basic technologies such as the installation and setup of desktop or laptop computers, data storage hardware, or business productivity software. As technologies become more sophisticated, such as the use of enterprise software applications, wireless networking or the use of mobile phone applications, the firms tended to use external resources.

A number of firms used both internal and external resources to implement some of the technologies. It was observed that

companies often used external resources to initially implement the technology, and then tended to use internal resources to maintain and upgrade the implemented technologies. This shows that most of the Nigerian business enterprises have resources to implement basic ICT; however, they lack skills and resources in more advanced/specialty functions such as ERP, and data storage and network solutions and utilized external help in these areas of ICT. This further emphasizes the need for ICT training amongst companies in Nigeria. Harindranath et al. [45] and [46] also found that the lack of ICT expertise was one of the main barriers in their study.

Discussion And Implications Of The Results

The analysis revealed that organizations in Nigeria are taking a comprehensive approach to their ICT investment, focusing on both strategic and operational aspects of their businesses. The impact has resulted in changes that include the enrichment of the ICT culture among employer and employee, and better accessibility to information.

This analysis also revealed that companies in Nigeria are making significant investment in ICT and there is a low competition amongst companies in the marketplace. The main driving forces for ICT investment were to provide better and faster customer service, and to stay ahead of the competition. The study found that about two-thirds of the respondents have realized business benefits of ICT adoption such as better customer relationships, increase in revenue and in reducing costs. About 80% of the respondents are very positive about increasing their business performance in the future.

With regard to barriers to ICT investment, the majority of firms felt that a lack of necessary internal skills and high costs of implementation were the major barriers. More than half of the respondents felt that the costs of implementation were too high. Lack of availability of relevant information and advice on suitable and effective technologies was also one of the major barriers. Other barriers included companies having no time to implement ICT projects, lack of top management support, negative past experiences, and adhering to government regulations and requirements. These findings were consistent with other studies [45][29].

Overall, 89% of the surveyed organizations outsource some portion of their ICT functions. More than one quarter of the participants outsourced over half of their ICT activities. This can be related to the lack of in-house capabilities in ICT identified as a major barrier. These results also confirm findings of [45][29][46] and re-emphasizes the need for ICT training in business enterprises. The findings of our research show that the surveyed companies lacked necessary ICT knowledge and skills as well as the mechanism to find and receive advice and support. Our study found that Nigerian firms have adopted basic technologies (computers, productivity software, internet, and accounting and HR packages) but are limited in the more sophisticated technologies such as wireless, data storage, and network security solutions, ERP, CRM, SCM and E-Commerce. In order for Nigerian organizations to move to the next level of ICT adoption, and to be more competitive it is suggested that the Nigerian government:

- Should increase awareness among SMEs of the benefits of ICT adoption in order for them to become more competitive;
- Develop policies, procedures, standards, and guidelines for the various sectors of the ICT industry; provide incentives for ICT adoption in the form of soft loans, or special arrangements with vendors to

provide ICT products and services at affordable prices; and allocate more resources to upgrade the telecommunication infrastructure within the country

Additionally, organizations in Nigeria could become more competitive by investing more in the training of their employees in ICT. Finally, trade organizations (Ministry of Trade & Investment and the Chamber of Commerce) could establish special departments to focus on providing up-to-date information on appropriate ICT solutions to SMEs and to provide consulting services at no cost or at a very low cost on ICT adoption.

Conclusion

The study provides an overview of the current status of ICT adoption in private and public organizations in Nigeria. The analysis revealed that Nigerian companies are focusing on both strategic and operational aspects of their business. The impact has resulted in changes thatinclude the enrichment of the ICT culture among employer and employee, and better access to information. This study revealed that organizations in Nigeria have made a significant investment in ICT to date. There is relatively little competition amongst companies in the marketplace. The majority of the respondents have realized business benefits from ICT adoption such as better customer relationships, increase in revenue and cost reduction. The main drivers for ICT investment were to provide better and faster customer service, stay ahead of the competition, and follow management directives. Lack of internal skills and the high costs of ICT were the major barriers in adopting ICT. An important contribution of this paper is that it provides preliminary exploratory data on the various aspects of ICT in Nigerian organizations. The findings of this research will provide a foundation for future research and will help policy makers in understanding the current situation regarding usage and the impact of ICT on companies in Nigeria.

Limitations of the Research and Directions for Future Research

This study was a preliminary exploratory study to learn about the status of usage and adoption of ICT in enterprises in Nigeria. There are a number of issues such as legal, regulatory, interventions from the government in the adoption of ICT that require further investigation. These results are based on a sample of 102 companies. Data was collected from Nigerian companies who use some form of ICT in their business thus the vast majority of businesses in Nigeria who do not use computers (mainly micro business) were excluded from the research sample. The results show a general trend and practices of the use and impact of ICT on business enterprises in Nigeria. A larger sample is needed to further validate these results and trends

.

References

[1] Papaioannou, S.K.(2004). *FDI and ICT Innovation Effect on Productivity Growth: A Comparison between Developing and Developed Countries*, Athens University of Economics and business, Athens , Greece.

[2] Van Dijk, J. (2006). *The Network Society.* 2nd Edition, London: SAGE.

[3] Burke, K. (2010). The Impact of Internet and ICT Use among SMË Agribusiness Growers and Producers, *Journal of Small Business and Entrepreneurship*, 23(2), 173-194.

[4] Limi, A. (2008). Effects of Improving Infrastructure Quality on Business Costs: Evidence from Firm-Level Data, Policy Research Working Paper 4581, World Bank, Washington, DC.

[5] Piatkowski, M. (2003). The Contribution of ICT Investment to Economic Growth and Labor Productivity in Poland 1995-2000: http://ideas.repec.org/p/wpa/wuwpdc/0308002.html

[6] Clift, S. (2003). E-Democracy, E-Governance and Public Net-Work.

[7] Oliner, S.D. and Sichel D. (2004). The Resurgence of Growth in the Late 1990s: Is Information Technology the Story? *Journal of Economic Perspectives*, 14(4), 3-22.

[8] Mohr, J.J. and Shooshtari, N.H. (2003). Introduction to the Special Issue: Marketing of High Technology Products and Innovations, *Marketing Theory Practice*, 11(3), 1-12.

[9] Nour, S.S.O.M. (2006). ICT Opportunities and Challenges for Development in the Arab Region. In: D'Costa, A.P. (ed.) The New Economy in Development: ICT Challenges and Opportunities, 161-187. http://ec.europa.eu/enterprise/policies/industrial-competitiveness/industrial- http://www.publicus.net/articles/edempublicnetwork.html policy/files/communication_on_industrial_policy_en.pdf Technology Manager in Saudi Arabia, Ph.D. Thesis, University of Manchester. www.init.org.pk/papersandpublications/P4.pdf

[10] Nour, S. (2008). The Use and Economic Impacts of ICT at the Macro-Micro levels in the Arab Gulf Countries, Paper prepared for the Fifth GLOBELICS Academy, TaSTI, University of Tampere, Tampere, Finland.

[11] El-Shenawy, N. (2010) ICT Measurement: Egypt's Experience, First Workshop of the Regional Project "ICT Indicators and Capacity Building for ICT Measurement in Arab Region", Amman, 25-27 Sept.

[12] European Commission (EC) (2010). An Integrated Industrial Policy for the Globalization Era Putting Competitiveness and Sustainability at Centre Stage.

[13] Pettey C. & Tudor B. (2011). Gartner Says Worldwide IT Spending to Grow 5.1 Percent in 2011. http://www.gartner.com/it/page.jsp?id=1513614

[14] Bayly, C.A. (2004). *The Birth of the Modern World*, 1780-1914, Oxford: Blackwell.

[15] The World Bank (2006). Information and Communications for Development. Washington, D.C.:http://ppi.worldbank.org

[16] Roeller, L. and Waverman, L. (2001). Telecommunications Infrastructure and Economic Development: A Simultaneous Approach, *American Economic Review*, 91(4), 909-923.

[17] Hamilton, J.(2000). Institutions, Competition and the Performance of Telecommunications Infrastructure in Africa, PURC working paper, University of Florida, Gainesville, USA.

[18] Shirazi, F. (2008). The Contribution of ICT to Freedom and Democracy: An Empirical Analysis of Archival Data on the Middle East, *The Electronic Journal on Information Systems in Developing Countries*, 35(6), 1-24.

[19] Jelassi, T. (2010). ICT in Tunisia: A Strategic Lever for Building a Knowledge-based Economy, in Soumitra Dutta and Irene Mia (Editors): The Global Information Technology Report 2009-2010: ICT for Sustainability, World Economic Forum and INSEAD, March, 153-164.

[20] Shih, E., Kraemer, K.L. & Dedrick, J. (2008). IT Diffusion in Developing Countries, *Communications of the ACM*, 51(2), 43-48.
[21] ITU (2010). International Telecommunications Union: http://www.itu.int/en/pages/default.aspx
[22] Pisciotta, A. A. (1997). Global Trends in Privatisation and Liberalization. In: W. Melody (ed.) *Telecom Reform: Principles, Policies and Regulatory Practices*, Lyngby: Den private Ingenirrfond, Technical University of Denmark.
[23] Wellenius, B. (1999). Mitigating Regulatory Risk in Telecommunications (Note No. 189), in Public Policy for the Private Sector. Washington, D.C.
[24] Bortolotti, B., D'Souza, J., Fantini, M. and Megginson, W.L. (2002). Privatization and the Sources of Performance Improvement in the Global Telecommunications Industry, *Telecommunications Policy*, 2, 6, 243-268.
[25] Heeks, R. (2002). Information Systems and Developing Countries: Failure, Successes, and Local Improvisations, *The Information Society*, 18(2), 101-112.
[26] Bodla, M.A. and Rashid, M.A (2005). Technology Adoption in Islamic World: Problems and Prospects, International Conference on Contemporary Issues in Information Technology in OIC Member States, organized by INNIT (Inter-Islamic Network of Information Technology) on July 26-27, at Marriot Islamabad – Pakistan.
[27] Mofleh, S. Wanous, M. and Strachan, P. (2008). Developing Countries and ICT Initiatives: Lessons Learnt from Jordan's Experience, *The Electronic Journal on Information Systems in Developing Countries*, 34(5), 1-17.
[28] Kapurubandara, M. (2009). A Framework to e -Transformation SMES in Developing Countries, *The Electronic Journal on Information Systems in Developing Countries*, 39(3), 1-24.
[29] Mohammed, R. & Moruf, M. (2008). Use and Impact of ICT on SMEs in Libya. *The Electronic Journal of Information Systems Evaluation,* 11, 3, 125-138.
[30] Booz & Co (2010). Fast, Lean, and Agile: How GCC Governments Can Make the Most of ICT Investments, http://www.booz.com/media/uploads/Fast_Lean_and_Agile.pdf.
[31] Abdallah, S. and Al-badri, F. (2011). A Perspective on ICT Diffusion in the Arab Region. In: S. Abdallah & F.A. Ahmad. (Eds.) ICT Acceptance, Investment and Organization: Cultural Practices and Values in the Arab World, *IGI Global*, Chapter 1, 1-15.
[32] Hamade, S.N. (2009). Information and Communication Technology in Arab Countries:Problems and Solutions, in the proceedings of: New Generations, 6th Conference on Information Technology, Las Vegas, NV, USA, 27-29 April, 1498-1503.
[33] Yahia, M. (2011). Information and Communication Technologies on the Rise in the Gulf States. www.nature.com/nmiddleeast/2011/110504/full/nmiddleeast.2011.53.html
[34] Anyakoha, M.W. (1991). *Basic librarianship: Modern Technologies in Information work*. Owerri: Totan publisher, Pp. 106-108.
[35] Hawkridge, D. (1983). New Information Technologies in Education. London: Broom Relm, P. 161.
[36] UNDP (2001). World report on human development 2001. United Nations

Development Programme. De Boeck University for UNDP, Brussels, Belgium.

[37] Crede, A., & Mansell, R. (1998). *Knowledge societies in a nutshell: Information Technologies for Sustainable Development*. Ottawa, Canada: IDRC.

[38] Ndukwe, E. (2002). Application of Information Technology. The Pointer, 28 October, P.16.

[39] Federal Republic of Nigeria (2001). Nigeria National Policy on Information Technology (IT). Available: www.nitda.gov.ng/nigeriapolicy.pdf.

[40] Gable, G.G.(1994). Integrating Case Study and Survey Research Methods: An Example in Information Systems, *European Journal of Information Systems*, 3(2): 112-126.

[41] Remenyi, D. & Williams, B. (1995). Some Aspects of Methodology for Research in Information Systems, *Journal of Information Technology*, 10(3), 191-201.

[42] Al-Assaf, Y. (1997). Computer-Based Information Systems in the Role of Information

[43] Al-Shuaibi, A. (1998). The Impact of Information Technology on Organizations: The Case of Saudi Private Sector, Ph.D. Thesis, University of St Andrews.UK.

[44] Pritchard, S. (2006). How Can So Many Businesses Cope without Computers? *Financial Times*, 1(9),19.

[45] Harindranath, G., Dyerson, R. and Barnes, D. (2008). ICT Adoption and Use in UK SMEs: A Failure of Initiatives? *The Electronic Journal of Information Systems Evaluation*, 11(2), 91-96.

[46] Chibelushi, C. (2008). ICT Industry Challenges in Adopting ICT: A Case Study from the West Midlands, UK. In: proceedings of the 2008 International Conference on Information Resource Management, 18-20 May, Niagara Falls, Canada.

A Framework for Effective Software Monitoring in Project Management

[1]Wemembu, Uchenna Raphael, [2]Okonta, Okechukwu Emmanuel [3]Ojugo, Arnold Adimabua
[4]Okonta, Imah Love

[1]Department of Mathematics Federal College of Education. (Tech) Asaba.
[2] Department of Computer Science Federal College of Education. (Tech) Asaba
[3] Department of Math/Computer Science, Fed University Petroleum Resources Effurun
[4] Department of Technical Drawing Federal College of Education (Tech) Asaba.

Abstract

Developed software for project management rely heavily on collecting metrics to provide the progress feedback necessary to allow control of the project; however, interpretation of this data is very difficult and sometimes cumbersome. This paper addressed the need of a software implementation progress model that is needed to help interpret the accumulated data. Certain criteria are set for design of a proposed implementation progress model. Some findings from the studied projects from other researchers suggest the model is consistent with the observed behaviour. In addition to quantitative validity, the model is shown to provide meaningful interpretation of collected metric data by embedding certain quality function.

Key words: Project Management, Feedback, project control, metrics, process model, quantitative validity

---

Introduction

Developing software for effective project management in modern times rely heavily on periodically collected software metric data and this in turn used to provide management with feedback about the project, the process used and the stages in development. Metric data is most commonly used in the area of quality assessment and assurance. Well-defined metrics usually provide report on quality attributes such as anticipated number of faults remaining. But other areas, such as implementation progress and system throughput, hardly utilize feedback from Metrics data. Although, the total lines of source code, could be used to report on implementation progress but such measures have not been leveraged as strongly as quality assessment and assurance have been used.

Metric data is widely regarded as a valuable management feedback tool, yet it is generally not used to monitor implementation progress. An implementation progress model is presented and shown to identify project phase boundaries, express the rate of implementation during each phase, and allow objective comparisons between projects. This paper provides a framework to help interpret periodically collected implementation data. This work develops a model for interpreting implementation progress. The proposed progress monitoring model uses existing implementation artifact metrics, tries to match our understanding of the implementation progress, and allows project evaluation based on estimation of parameter used .Well-defined and proven metrics exist for many areas of software

engineering and development including especially quality assessment and assurance. Implementation progress has no such established metrics.

The lack of proven implementation progress metrics has been a barrier to any attempt to effectively monitor project development. Nevertheless, this shortcoming is not insurmountable. Size metrics are abundant and deriving a progress metric
from a size metric can be accomplished by working out the difference in consecutive size measurements. A far larger barrier than the lack of a metric is the lack of a proven implementation progress *model*. Periodically collected data is rich in detailed information but is not in itself meaningful. A model provides a specific interpretation of the data and allows meaning to be extracted. An implementation progress monitoring model will allow periodically collected implementation data to be effectively interpreted.

Several existing metrics measure size-related attributes. While these size-related metrics may have been originally developed to support quality assessment and assurance, they can be used to monitor progress in terms of size. Project size is important because it is usually used to estimate the resources needed and therefore assess the project's status with regard to the schedule for completion [6]; [1]; [16]. This known fact about management need for feedback about implementation progress should demand its use because its absence may be as result not introducing metrics to support implementation progress monitoring feedback before now.

Basic Concept

We design models normally to bridge the gap between real sampled data and expected outcomes. In real terms models act as predictors to set expectations over the next few data samples but in a small scale. Take for instance a defect model, this may indicate the number of faults to be found in a released project and the degree to which the actual number of faults discovered differs from the predicted value can actually be an indication of unexpected circumstances within the project. This means that, an unusual low value may be pointing to the fact that fewer code changes were made than expected, or that less testing was carried out than expected. This also means that Management has been forewarned; an investigation can be made and then appropriate response taken. This feedback, though small scale provides valuable and timely feedback to the management within the scope of the executing project.

In addition to this small scale feedback, models provide feedback on a larger scale, where the feedback focuses more on the overall picture portrayed by the data. This is regularly required by management, with or without a formal model. Without a formal model management team must rely on guess work. In contrast to this unusual approach, a formal model can be adopted to establish a rigorous evaluation. A formal model establishes the critical parameters within the system. Using a formal model, projects may be evaluated or compared in terms of the model parameters. Model parameters allow evaluation and comparisons to be based on defendable data rather than guess work and hearsay. Additionally, given estimated values for the parameters, the model can make predictions about the outcome. This relationship between parameters (input) and predictions (output) codifies a causal effect believed to be true within all designed system.

Similar Research Done Before Now

Some work done before with reference to software metrics on the development process has been directed at tasks before and after implementation. Much work has been done in the pre-implementation stages to improve effort prediction and estimation [1]; [22] [16]; [5]; [36]. Metrics

have also been used to evaluate architectural design before implementation. Significant work has been done in the post-implementation stages to predict failure rates, both for a project as a whole as well as for individual modules [15]; [11]; [37]; [9]; [34].

However, substantially less work has been published regarding the use of metrics for assessment, monitoring, or control of the implementation stage itself. DeMarco confirms this when he asserts "you can't control what you can't measure" [6]. In fact, every researcher now that is proposing, defending, or merely discussing a metric agrees the reason behind metrics and measuring is to gain some degree of understanding and control over the complex process of software development [10]. Recent studies have focused attention on *how* to use the vast array of data generated by existing measures.

Some published works emphasizing how to use the potentially enormous data available can be coarsely divided into three groups. Many works assert metrics should be used to assist in monitoring, evaluation and control of projects during the implementation phase [6]; [3]; [4]; [23]; [37]; [19]. Other researchers recommend specifically that time-series metrics data be used to monitor and evaluate projects [6]; [28]; [34]. The last group that consist of several researchers emphasize the idea gained from causal models over correlative models [32]; [10]; [36]. They suggest models which provide an inherent causes-relationship are more valuable than simpler correlation models.

Model Design

The main purpose of designing a model is to provide a documented method of interpreting a set of data. In most cases the interpretation is usually obscured by the sheer quantity and detail of the enormous data available and Information can only be revealed when these data are interpreted in a particular way. The interpretation results can then be used to evaluate past performance, assess the current situation, and make predictions about future performance.

The interpretation can also be used to compare multiple data sets. Results from the same model, applied to several data sets, allow the data sets to be easily compared in terms of the model. The model provides a systematic method for comparing projects. One type of model interprets series data by attempting to fit collected data to a family of curves. The single curve which best fits the data is used to describe the data in terms of the model. The specific values used to generate the best fitting curve are considered parameters of the model. Parameters of a model reveal one or more dimensions of the collected data. In this case, parameters can be considered an output of the model. Collected data is the input and results summarizing that data are produced. Parameters can also be used as input resulting in expected sample data. When used in this way, models make predictions based on estimated parameters. In either case, the expected progress as defined by the model is given by the model curve.

The model equation and a specific set of parameters define the model curve.

A valuable model is one that produces a clear and concise interpretation of the data. Part of this interpretation is in the form of the specific values for the model parameters. For example, consider two models, one uses only two parameters while the other has eight parameters. Even though the eight-parameter model may predict the data "twice" as well, it may not be the better model if its parameters have no particular meaning or are hard to estimate. Models should have as few parameters as possible while still modelling the data with sufficient accuracy. Fewer parameters means the model is easier to understand.

Part of understanding a model is understanding the relationships between the

parameters. Parameters are related by the effects each has on the others. Knowing the trade-offs between parameters is necessary to understand a model. This is easier if the model contains fewer parameters. In addition to relatively few parameters, individual model parameters should be understandable. Understandable parameters produce simple results with meaning.

On the other hand, meaningless parameters do not help to simplify or interpret the data since they must again be interpreted. Parameter meaning is even more important when the model is used as a predictor for new projects. In this case, model parameters must be estimated before any data has been collected. If the individual parameters are well understood better estimates for each will be made. Better estimates will produce better predictions. Related to individual parameter meaning is the parameter unit. Model parameters should be expressed in well-known units, rather than new or arbitrary ones. Parameters with direct interpretations allow the model results to be easily understood and used. Well-known units are also much easier to estimate. Again, this allows for better predictions. Model parameters should be few in number, directly interpretable, and measured in existing units. These properties give the model parameters the most meaning and thus give the model the most "clarifying power".

Implementing Model's Monitoring.

Generally, Implementation progress is not a new concept and so in addition to basic model requirements, an implementation progress model must be compatible with existing models. An informal progress model already exists; it can be seen in project vocabulary and assumptions. For instance, this informal model is commonly used to answer certain project status queries, such as:

What is the expected completion date based on the current pace?
What was the size of the total effort for that project?
What fraction of the total effort is currently done?
What fraction of the total effort will be done by a certain date?

A proposed framework implementation model should serve the same purpose as the informal model. The model must help provide answers to questions about implementation speed and progress of current and future projects. The informal progress model captures another key attribute of implementation progress. The informal model acknowledges that project speed is not constant throughout a project: because sometimes projects "speed up" and "slow down". There must always be the ability or desire to constantly determine implementation velocity. As noted by (McConnell 1998) this velocity increases at the beginning and decreases near the end. A formal implementation progress model should be informed by this experience and capture the canonical variations in velocity during implementation.

In a nut shell, the desired attributes of a formal implementation progress model include relatively few parameters, understandable parameters, well-known parameter units, consistency with informal progress model, and the ability to answer management questions involving size and velocity.

Evaluation And Control

DeMarco presents a development process relying on steadily improving estimates to provide feedback and control during all phases of software development[6]. Metrics collected at each stage of development provide raw data for creating an improved estimate for the next stage. Metrics from the current project as well as previous projects are used to make inform decisions. What was focus

throughout his work is the need for continuing feedback by continuously improving estimates while allowing the development effort to be properly directed. He made a compelling case supporting estimates reviews, process metrics, and cost models in order to make quality improvement. DeMarco identifies and recommends appropriate metrics for each stage of development.

In discussing appropriate metrics for the implementation stage DeMarco points to process metrics such as *compilation rate* but did not explore them. The primary implementation measure is *code weight,* which is defined as a product of two dimensions: size and complexity. DeMarco defines code size as information content within a program. He recommends using Halstead's volume metric [12] to find size. Several alternatives for measuring complexity are presented, but McCabe's cyclomatic complexity measure [27] was recommended. Using these two dimensions as parameters, an algorithm is presented for computing *implementation weight.* Historical data from similar projects and environments is also used to provide scaling factors. According to DeMarco, the primary motivation for computing implementation weight is to improve future project estimates. However, he also calls it a "project predictor", as it was deplored to predict the final size of the project accurately. According to this novel system presented by DeMarco, the measure should be taken once near the middle of implementation. However, progress model been proposed by this paper may provide a better estimate of implementation size. Since the proposed model considers the complete project history, not simply a single point in time, because this is less prone to errors.

Boehm considered a broader approach to development feedback than simply focusing on improved estimates. He introduces a software development methodology whose principal aim is risk management [4]. His spiral model of software development relies on risk evaluation as the impetus for each unit of work, whether the work unit is a prototype, design document, or code. Risk management implies the ability to control what is being managed. This agrees with DeMarco's argument that our need to measure the software development process stems from our desire to control the process [6]. Boehm's methodology assumes feedback metrics exist to inform the risk evaluation process, but does not dictate specific measures or measurement processes.

Addressing the selection of appropriate metrics for quality control, Solingen and Berghout defined the Goal/Question/Metric Method (GQM) of improving software quality [37]. Goal/Question/Metric Method integrates metrics into the development process in order to answer questions about quality raised by corporate goals. Their methodology relies on the ability to follow the connection between corporate goals and specific metrics, in both directions. Measurements are defined by goals and the results interpreted in terms of those goals. In the area of quality control, well developed process models exist to help define and interpret metrics. However, implementation models in general, and implementation progress in particular, have not been well developed.

Kirsopp addresses the need to capture development models and enough datato evaluate them. He strongly argues that the software development process needs measurements for feedback and that the integration must be close, detailed and appropriate [19]. Organizations must support metrics outside of a single project in order to validate the process, validate the results, and collect historic data. All three of these are required to assist future project estimates. An *experience factory* provides a repository for captured experiences and models, allowing reuse ‘within an organization. Kirsopp cites the “Tailoring a Metric Environment” Project

[3] as a working example of an experience factory.

Lott provides an alternative approach; instead of suggesting or analyzing metrics, he studied several available and proposed software engineering environments [23]. Many of these environments include integrated tools for collecting numerous metrics about various development artifacts created. Lott suggests collected data can be used to guide development and to call attention to atypical patterns worthy of investigation. In this regard, he assumes time-series data will be collected and evaluated. Inherent in this idea is the development of a canonical pattern or typical shape for a particular metric. Unfortunately, neither Lott nor the systems studied define how to select or interpret the automatically collected measurements.

Time-Series Shape Metrics

Estimation is core to every software metrics consideration but in addition to that, DeMarco briefly notes that process metrics, such as compilation rate, can be used to identify project dysfunction and impending problems [6]. Periodic sampling of a metric allows the value measured to be graphed against time. For some measures, such as compilation rate, which means that all well planned projects, may all have similar shapes when viewed as time-series data. If this is the case, then projects not properly planned can be detected if or when they deviate from the canonical shape. Actually, DeMarco suggested that compilation rates that continue at a steady rate without showing any decline may be an indication of a poor work from development team. While this particular evaluation may not apply to all development environments, the idea of a well planned project canonical shape can be applied to all environments.

In another breathe, he recommended reporting test progress as a graph showing measurements against time. Time-series graphs make it clear how test progress has been proceeding and how its trends change over time. In general, comparing the current project with similar historic projects using graphs can highlight abnormal trends which may be an indicator of trouble. Given DeMarco's emphasis on continuous monitoring and improvement, it is surprising he does not suggest using implementation artefact metrics, such as size or complexity, to monitor implementation progress.

Schneidewind used time-series metrics to create a method for evaluating process stability [34]. Schneidewind emphasizes that metric trends are a significant indicator of the underlying process and monitoring the trends can provide feedback about the process. To quantify these trends, he introduces two new classes of indirect metrics. A *change metric* is computed using differences in consecutive values of a traditional metric. This metric can be viewed as the derivative of the primary metric. The other class of indirect metric introduced is the *shape metric.* A shape metric is derived from the curve of the time-series metric data when graphed against time. For example, one shape metric suggested is the time at which the failure rate is highest. Lower values for this metric may indicate process stability, while higher values may indicate instability in the development process. A strong case is presented for the use of time-series data, and indirect metrics derived from it, in the context of process stability. Monitoring progress during the development stage using change and shape metrics is an obvious extension of this study.

McConnell understands typical "code growth" on a project to contain three distinct phases [28]. In the first phase, architectural development and detailed design generate very little code. The second phase provides staged deliveries and includes detailed design, coding, and unit testing. During this phase code growth is very high. During final release, the third phase, code growth slows to a crawl. McConnell shows a graph depicting a

typical code growth pattern for a well-managed project. He indicates the phase transitions occur at approximately 25% and 85% of the total development time, but acknowledges that this varies to some degree. His main point is periodic monitoring of code size is a valuable feedback tool for managers. No details are given about the specific metric(s) involved or the process used to collect the data. The proposed progress model clarifies how metrics are used and provides a specific interpretation of the three phases documented by McConnell.

Process Models

Powell expanded the frontier of the role of software measurement to explicitly include not only prediction and control but also assessment and understanding [32]. He propounded arguments for assessment similar to those presented by Boehm and DeMarco for prediction and control. Regardless of the motive, measurements are always based on assumptions about the process in which the measurement is taken. Powell states "it is impossible to talk about measurements without implying some form of [process] model" [32]. Before measurements can be taken, and before metrics can be determined, a model of the development environment must be chosen.

Turski presents a model for understanding the observed rate of software growth as a function of time [36]. Using the number of modules as the dependent variable and uniform inter release intervals as the independent variable, he shows size correlates strongly with the third root of time {size = \/time). While defendable on the bases of Lehman's Laws of Software Evolution [21], Turski uses a simple mental model to understand the same relationship. He suggests envisioning a system as a sphere with "surface" modules being easy to modify while "interior" modules are much harder to modify. With this model in mind, it is easy to see that the proportion of easy modules to hard modules tends toward zero as the project (sphere) grows with time.

Turski believes that simple and manageable models provide powerful insights into understanding the forces at work in software development. In particular, models which exhibit causal relationships rather than simple statistical correlations provide not only better interpretation but improved understanding of the process.

Framework Design

Project managers and software designers have developed an actual framework from intuition about what should occur during a software development process. And as a matter of fact framework implementation progress model should be consistent with this acquired experience. A condensed version of this collective wisdom is presented by McConnell [28]. He uses *code growth* as a measure of progress and provides a nominal code growth pattern as well *as* a range of normal variations for well-run projects. An appropriate progress model should reflect the basic shape of accepted norms such as those presented by McConnell.

Another constraint on designing an appropriate framework implementation progress model is its interpretive power. Interpretation of metric data relies on some understanding of the underlying process and how it works. Take for instances, changes in the rate of progress in an otherwise stable environment may indicate the project has transitioned to a new phase. This assumes the rate of progress is dependent on the project state. This process of drawing meaning from data, such as when a phase ends, is interpretation and of course an implementation progress model must approximate actual project data collected.

Solution Model:

Static Analysis

Halstead's Software Physics or Software Science

n1 = no. of distinct operators in program
n2 = no. of distinct operands in program
N1 = total number of operator occurrences
N2 = total number of operand occurrences
Program Length: N = N1 + N2
Program volume: $V = N \log_2 (n1 + n2)$

(represents the volume of information (in bits) necessary to specify a program.)

Specification abstraction level: L = (2 * n2) / (n1 * N2)
Program Effort: $E = (n1 + N2 * (N1 + N2) * \log_2 (n1 + n2)) / (2 * n2)$

(interpreted as number of mental discrimination required to implement the program.)

McCabe's Cyclomatic Complexity

Hypothesis: Difficulty of understanding a program is largely determined by complexity of control flow graph.

- Cyclomatic number V of a connected graph G is the number of linearly independent paths in the graph or number of regions in a planar graph.

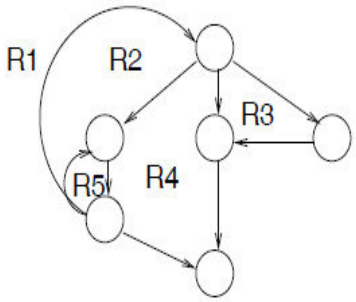


Fig. 1: Planar Graph

- Claimed to be a measure of testing difficulty and reliability of modules.
- McCabe recommends maximum V(G) of 10.

Static Analysis (Problems)

- Doesn't change as program changes.
- High correlation with program size.
- No real intuitive reason for many of metrics.
- Ignores many factors: e.g., computing environment, application area, particular algorithms implemented, characteristics of users, and ability of programmers.
- Very easy to get around. Programmers may introduce more obscure complexity in order to minimize properties measured by particular complexity metric.
- Size is best predictor of inherent faults remaining at start of program test.

Bug Counting Using Dynamic Measurement

Estimate number remaining from number found.

1) Failure count models 2) Error seeding models

Assumptions:

- Seeded faults equivalent to inherent faults in difficulty of detection.
- A direct relationship between characteristics and number of exposed and undiscovered faults.
- Unreliability of system will be directly proportional to number of faults that remain.
- A constant rate of fault detection.

What does an estimate of remaining errors mean?

- Interested in performance of program, not in how many bugs it contains.
- Most requirements written in terms of operational reliability, not number of bugs. Alternative is to estimate failure rates or future inter -failure times.

Estimating Failure Rates

Input-Domain Models:

- Estimate program reliability using test cases sampled from input domain.
- Partition input domain into equivalence classes, each of which usually associated with a program path.

- Estimate conditional probability that program correct for all possible inputs given it is correct for a specified set of inputs.
- Assumes outcome of test case given information about behaviour for other points close to test point.

Reliability Growth Models

Software Reliability: The probability that a program will perform its specified function for a stated time under specified conditions.

- Execute program until "failure" occurs, the underlying error found and removed (in zero time), and resume execution.
- Use a probability distribution function for the inter failure time (assumed to be a random variable) to predict future times to failure.
- Examining the nature of the sequence of elapsed times from one failure to the next.
- Assumes occurrence of software failures is a stochastic process.

Software Uncertainty

Assumption: The mechanism that selects successive inputs during execution is unpredictable (random). O is the image set of I_F under the mapping p

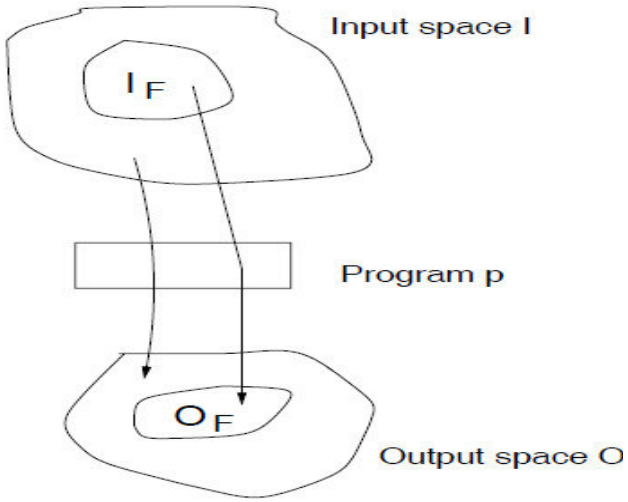


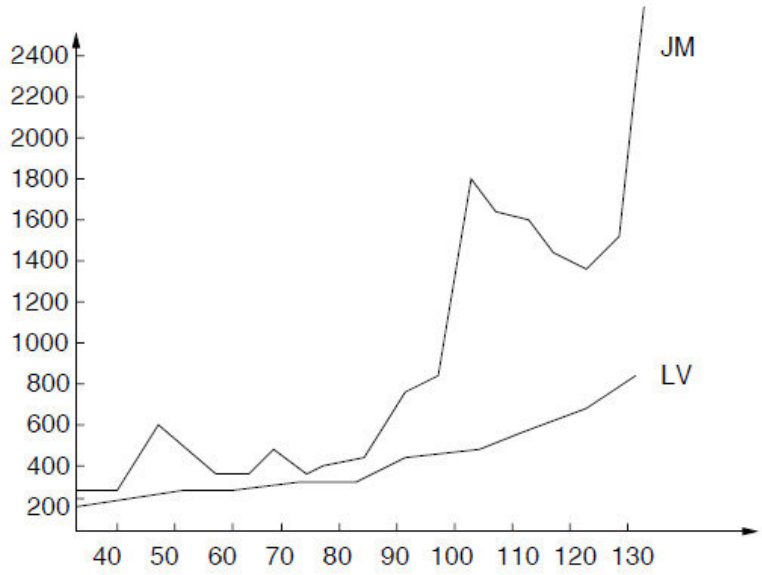
Fig. 2: Software Uncertainty illustrated

Table 1: Sample Inter Time Data

3	30	113	81	115	9	2	91	112	15
138	50	77	24	108	88	670	120	26	114
325	55	242	68	422	180	10	1146	600	15
36	4	0	8	227	65	176	58	457	300
97	263	452	255	197	193	6	79	816	1351
148	21	233	134	357	193	236	31	369	748
0	232	330	365	1222	543	10	16	529	379
44	129	810	200	300	529	281	160	828	1011
445	296	1755	1064	1783	860	983	707	33	868
724	2323	2930	1461	843	12	261	1800	865	1435
30	143	109	0	3110	1247	943	700	875	245
729	1897	447	386	446	122	990	948	1082	22
75	482	5509	100	10	1071	371	790	6150	3321
1045	648	5485	1160	1864	4116				

Applying the Models

Different models can give varying results for the same data; there is no way to know a priori which model will provide the best results in a given situation



.

Fig. 3: Models Applied

The nature of the software engineering process is too poorly understood to provide a basis for selecting a particular model."

Software Design Metrics

Number of parameters

- Tries to capture coupling between modules.
- Understanding modules with large number of parameters will require more time and effort (assumption).
- Modifying modules with large number of parameters likely to have side effects on other modules.

Number of modules

Number of modules called (estimating complexity of maintenance).

Fan-in: number of modules that call a particular module.

Fan-out: how many other modules it calls.

- High fan-in means many modules depend on this module.
- High fan-out means module depends on many other modules.

Makes understanding harder and maintenance more time-consuming.

Data Bindings

Triplet (p,x,q) where p and q are modules and X is variable within scope of both p and q.

Potential data binding:

- X declared in both, but does not check to see if accessed.
- Reflects possibility that p and q might communicate through the shared variable.

Used data binding:

- A potential data binding where p and q use X.
- Harder to compute than potential data binding and requires more information about internal logic of module.

Actual data binding:

- Used data binding where p assigns value to x and q references it.
- Hardest to compute but indicates information flow from p to q.

Cohesion metric

Construct flow graph for module.

- Each vertex is an executable statement.
- For each node, record variables referenced in statement.

Determine how many independent paths of the module go through the different statements.

- If a module has high cohesion, most of variables will be used by statements in most paths.
- Highest cohesion is when all the independent paths use all the variables in the module.

Robert Cecil Martin Popularized Software Package Metrics

Robert Cecil Martin is one of the creators of agile software development methodologies and extreme programming. Created metrics used for evaluating object oriented software packages which was also meant to be used with in an extreme programming framework. The advantage is that the metric calculation is relatively transparent.

As long as the criteria are important, developers can build software that follows these constraints and get better metrics about their code various aspects of software packages can be measured such as [4]

This metric shows how the package balances between abstractness and stability. A package will do well in this metric by being either mostly abstract or stable, or completely concrete and instable. Package dependency cycles: packages in the packages hierarchy that depend on each other. (Dependency cycles)

Embedding Quality

When fault prediction is incorporated in Robert Cecil Martin models it will allow organizations to predict defects in code before software has been released.

There is debate around aggregating the models or modelling only some of the defects more accurately. Part of the debate stems from the need for more research in software decomposition and how to decompose software for better quality systems. .Models are used to explain aspects of a software system numerically in at a statistically significant level. Research that is trying to address the human judgment side of metrics processing is also being addressed

Breaking down the defects that software is measured for will give a better view of the particular type of defect you are interested in and with the design Frameworks it is easy to understand metrics and making sure that we are using them correctly. Though the metrics analysis techniques, and the usefulness of data is not fool proof. Software metrics are statistical predictions and estimations, and not just a number. The numbers have three dimensions [2] error, bias, and variance or scatter. A human typically ignores these dimensions for simplicity and with the loss of information comes over optimism and over-confidence.

Research is being done to use meta cognition experiment results in application to software metrics interpretation and use in project planning and reflection. [2]. Researchers Carolyn Mair and Martin Sheppard want to include the perspective on how people actually employ software metrics results currently so they can understand how to make those metrics better. Kaner and Bond argue that metrics in software engineering are not yet properly used. In part this is because the validity of the metrics that are used is not emphasized.[10] .This could be due to many reasons, one being that software engineering is traditionally a empirical field. If the software is working the default action is typically to leave it alone.

Also, one of the most common form of software metrics is automated and user testing. This happens to be very expensive and one of the first things to get cut from the development lifecycle. So if a company or organization is going to cut testing, it seems likely to us that they would also not use metrics for the same reasons.

Conclusions

Few metrics have been demonstrated to be predictable or related to product or process attributes so interpreting implementation progress measurements is difficult. A simple model is needed to provide a framework to help interpret the data. We have developed a piecewise approximation based on a three-phase model of linear implementation velocity. The model corresponds well to our intuition of how project progress occurs. It identifies project phase boundaries as well as the velocity of implementation during each phase. Furthermore, the progress model allows objective comparisons of project velocity between projects and easily supports estimating.

The progress model fits the available sample data much better than a linear model. With only one additional degree-of-freedom, the model produces fits with approximately two-thirds less error than a linear fit. When compared with a polynomial fit, the progress model performs at least as well as a polynomial model which has one additional degree-of-freedom.

Limitations and Recommendation

The progress model presented here only considers non-maintenance Imple- mentation. Projects with clear delivery dates, after which continuing development is not planned, fall into this category. Projects in maintenance or under continuous development may not exhibit phases similar to projects with firm end dates. Any model is only as good as the data on which it is based. Errors were discovered in both dimensions of the sample data. Spurious data entries were occasionally introduced due to the check-in process used. Similarly, project billing information could have helped improve the quality of the time data collected.

There is "a strong tendency for professionals to display over-optimism and over-confidence"]

Arguments that simplistic measurements may cause more harm then good, ie data that is shown because its easy to gather and display [5]

There are arguments about the effects that software metrics have on the developers' productivity and well being

This research paper provides a sound basis for further study in this area. application of the progress model to continuous development projects should be investigated.

Again there should be further study to take advantage of the stability of the model for making predictions. Estimating project parameters such as final size, delivery date, development pace, etc. during implementation should be investigated. Similarly, the effect of project properties, such as number of engineers, experience level, domain familiarity, length of project, etc., on the model parameters should also be studied.

.

References

[1] Albrecht, A. J. and J. John E. Gaffney (1983, Nov). Software function, source lines of code, and development effort prediction: A software science validation. *IEEE Transactions on Software Engineering* 5(6), 639-648.

[2] Andersson, T., K. Enholm, and A. Torn. RMC a length-independent measure of software complexity. Reports on computer science and mathematics, Abo Akademi University.

[3] Basili, V. R. and H. D. Rombach (1988). The TAME project: Towards improve mentoriented software environments. *IEEE Transactions on Software Engineering 14 {6),* 758-773.

[4] Boehm, B. W. (1988). Spiral model of software development and enhancement. *IEEE Computer 21 {3),* 61-72.
[5] Boraso, M., C. Montangero, and H. Sedehi (1996). Software cost estimation: an experimental study of model performances. Technical Report TR-96-22, Universita di pisa, departmento di informatatica.
[6] DeMarco, T. (1982). *Controlling Software Projects Management, Measurement and Estimation.* Inglewood Cliffs, NJ: Yourdon Press.
[7] El-Eman, K. (2000, June). A methodology for validating software product metrics. Technical Report NRC/ERB-1076 44142, National Research Council Canada, Institute for Information Technology.
[8] Fenton, N. E. (1991). *Software Metrics: A Rigorous Approach.* London: Chapman and Hall.
[9] Fenton, N. E. and M. Neil (1999). A critique of software defect prediction models. *Software Engineering 25 {5),* 675-689.
[10] Fenton N. E. and M. Neil (2000, June). Software metrics: roadmap. In *Proceedings of the conference on The future of Software Engineering,* pp. 357-370. ACM Press.
[11] Goel, A. L. and K. Okumoto (1979, August). Time-dependent error-detection rate model for software reliability and other performance measures. *IEEE Transaction on Reliability RE-28{3),* 206-210.
[12] Halstead, M. H. (1977). *Elements of Software Science.* New York, NY: Elsevier Scientific.
[13] Henry, S. M. and D. G. Kafura (1981, Sep). Software structure metric based on information flow. *IEEE Transactions on Software Engineering* 7(5), 510-518.
[14] Huffman, D. A. (1952, Sep). A method for the construction of minimum-redundancy codes. *Proceedings of the Institute of Electrical and Radio Engineers 40(9),* 1098-1101.
[15] Jelinski, Z. and P. Moranda (1971). Software reliability research. In W. Freiberger (Ed.), *Statistical Computer Performance Evaluation,* pp. 465-484. Providence, RH: Academic Press.
[16] Jorgensen, M. (1995). Experience with the accuracy of software maintenance task effort prediction models. *IEEE Transactions on Software Engineering 21 {8),* 674-681.
[17] Kafura, D. and J. Canning (1985, Aug). A validation of software metrics using many metrics and two resources. In *Proceedings of the 8th International Conference on Software Engineering,* pp. 378-385.
[18] Kaner, C., Bond, W. (2004) Software Engineering Metrics: What Do They Measure and How Do we Know? *10th International Software Metrics Symposium*
[19] Kirsopp, C. (2001, Apr). Measurement and the software development process. In 1*2th European Software Control and Metrics Conference,* pp. 165-173.
[20] Lake, A. and C. R. Cook (1994, apr). Use of factor analysis to develop oop software complexity metrics. In *Proceedings Sixth Annual Oregon Workshop on Software Metrics.*
[21] Lehman, M. M., J. F. Ramil, R D. Wernick, and D. E. Perry (1997). Metrics and laws of software evolution-the nineties view. In *Proceedings of 4th International Symposium on Software Metrics,* pp. 20.
[22] Lind, R. K. and K. Vairavan (1989, may). An experiemental investigation of software metrics and their relationship to software development effort. *IEEE Transactions on Software Engineering 15{h),* 649-653.
[23] Lott, C. M. (1993, Oct). Process and measurement support in sees. *ACM SIGSOFT Software Engineering Notes 18{-i),* 83-93.
[24] Mair, C., Shepperd, M. (2011) Human Judgement and Software Metrics: Vision for the Future. *WETSoM'11* (May 24, 2011), Waikiki, Honolulu, HI USA.

[25] Marasco, J. (2002, August). Tracking software development projects. *Dr. Dobb's Journal.*
[26] Martin, R. D. and V. Yohai (2001). Data mining for unusual movements in temporal data. In *KDD Workshop on Temporal Data Mining.*
[27] McCabe, T. J. (1976, Dec). A complexity measure. *IEEE Transactions on Software Engineering* S(4), 308-320.
[28] McConnell, S. (1998). *Software Project Survival Guide.* Redmond, WA: Microsoft Press.
[29] Misirli, A., Caglayan, B., Miransky, A., Bener, A., Ruffolo, N. (2011). Different Strokes for Different Folks: A Case Study on Software Metris for Different Defect Categories.
[30] Nagappan, N., Ball, T. (2007) Using Software Dependencies and Churn Metrics to Predict Field
Failures: An Empirical Case Study. *IEEE First International Symposium on Empirical Software Engineering Measurement.*
[31] Park, R. E. (1992). Software size measurement: A framework for counting source statements. Technical Report CMU/SEI-92-TR-20, Software Engineering Institute, Pittsburgh, PA.
[32] Powell, A. L. (1998). A literature review on the quantification of software change.technical report YCS-98-305, University of York, Department of Computer Science.
[33] Robert Cecil Martin (2002) .http://www.sdtimes.com/link/34157
[34] Schneidewind, N. F. (1999, Nov). Measuring and evaluating maintenance process using reliability, risk, and test metrics. *IEEE Transactions on Software Engineering 25 {6),* 761-781.
[35] Strelzoff, A. and L. Petzold (2003). Revision recognition for scientific computing: theory and application. In *18th Annual Software Engineering and Knowledge Engineering Conference,* pp. 46-52.
[36] Turski, W. M. (2002, August). The reference model for smooth growth of software systems revisited. *IEEE Transactions on Software Engineering 28{8),* 814-815.
[37] van Solingen, R. and E. Berghout (1999). *The Goal/Question/Metric Method.* London: McGraw-Hifl Publishing Company.
[38] Vasilescu, B., Serebrenik, A., van den Brand, M. (2011). By No Means: A Study on Aggregating Software Metrics.
[39] WETSoM'11 (May 24, 2011), Waikiki, Honolulu, HI USA. Agile Software Development: Principles, Patterns and Practices. Pearson Education.
[40] Woodings, T. L. and G. A. Bundell (2001, April). A framework for software project metrics. In *Proceedings of the ESCOM 2001*

.

Addressing Software Engineering Issues In Real-Time Software Development Environment

[1]Uchenna Raphael, [2]Okonta, Okechukwu Emmanuel, [3] Wemembu, Uchenna Raphael , [3]imiere, E. E. , [4]Aghware Fidelis

[1]Department of Computer Science, Federal College of Education (Tech) Asaba.
[2] Department of Mathematics Federal College of Education (Tech) Asaba.
[3]Department of Physics Federal College of Education (T) Asaba.
[4] Department of Computer Science College of Education Agbor.

Abstract

Real-time systems are normally deployed in a wide range of application such as transportation systems, manufacturing process, process control, military, space exploration, and telecommunications. These systems must satisfy not only logical functional requirements but also physical properties such as timeliness, Quality of Service and reliability. The cross-cutting behaviours imposed by these functional properties and dependencies on operational characteristics such as hardware, Operating System and firmware platforms that are used; have traditionally led to hard-to-code, hard-to-understand and hard-to-change software that are engineered. In this research paper we have identified few software engineering issues in development of real time systems and provided brief description of each of those issues and strived to make serious effort to proffer creditable and functional solutions.

Key Words: Real time systems, logical functional requirements, Quality of Service, Reliability, software engineering issues

---

Introduction

Real-time computing is an enabling technology for many important application areas, including process control, nuclear power plants, agile manufacturing, intelligent vehicle highway systems, air-traffic control, telecommunications, multimedia, real-time simulation, virtual reality, medical applications, and military applications. In almost all safety-critical systems and many embedded computer systems are visible real-time systems. Further, real-time technology is becoming increasingly important and pervasive, e.g., more and more infrastructure of the world depends on it. Strategic directions for research in real-time computing involve addressing new types of real-time systems including open real-time systems, globally distributed real-time, and multimedia systems. For each of these, research is required in the areas of system evolution, the actual software engineering, the science of performance guarantees, reliability and formal verification, general system issues, programming languages, and education. Economic and safety considerations, as well as the special problems that timing constraints cause, must be taken into account in the solutions. [2]

In this research paper we will be surveying some research activities carried out in the field of Software Engineering with relation to Real-Time systems. A hard real-time

computer system is required to produce the intended result before a specified point of physical time, the deadline. This point of time is determined by the application the computer system is intended to service. The controlling real-time software must be designed to generate the correct behaviour of the computer both in the value domain and in the temporal domain to meet this application requirement. Since the temporal behaviour of the software depends on the performance of the computer hardware, software engineering for real-time systems must take into consideration the architectures and capabilities of the available computer hardware. It follows that the software design methods and architectures of real-time systems will be strongly influenced by the given hardware environment and consideration.
[1]
These are some of the software engineering issues we identified in development of real-time systems:

- Requirements Analysis
- Re-engineering
- Validation

Requirements Analysis

All engineering is about how to produce products in a disciplined process. In general, a **process** defines *who* is doing *what, when* and *how* to reach a certain goal. A process to build a software product or to enhance an existing one is called a **software development process**. A software development process is thus often described in terms of a set of activities needed to transform a user's *requirements* into a software system.

The client's requirements define the goal of the software development. They are prepared by the client (sometime with the help from a software engineer) to set out the services that the system is expected to provide, i.e. *functional requirements*. The functional requirements should state *what* the system should do rather than *how it is done*. Apart from functional requirements, a client may also have non-functional constraints that she/he would like to place on the system, such as the required response time or the use of a specific language standard. We must bear in mind about the following facts which make the requirement capture and analysis very difficult:

- The requirements are often incomplete.
- The client's requirements are usually described in terms of concepts, objects and terminology that may not be directly understandable to software engineers.
- The client's requirements are usually unstructured and they are not rigorous, with repetitions, redundancy, vagueness, and inconsistency.
- The requirements may not be feasible.

Therefore, any development process must start with the activities of capturing and analyzing the client's requirements. These activities and the associated results form the first *phase* (or sub-process) of the process called *requirement analysis*. The purpose of the requirement capture analysis is to aim the development toward the right system. Its goal is to produce a document called *requirement specification*. The whole scope of requirement capture and analysis forms the so-called *requirement engineering*.

High-level design of the computerized component of a critical system is not performed in a vacuum but strongly depends on models and assumptions regarding, besides device itself, the environment, the sensors and the actuators.

Therefore, writing the design specifications, from which the development of the device can start, is not the first activity of the development process, but must be the result of a preliminary phase whose purpose is to state, analyze, and prove the user requirements (typically stated very abstractly in terms of some safety or utility property) by modelling the system in its entirety, including the device and all the other components.

The modelling and analysis activities must be formal, to provide a support in dealing with complexity, to obtain mechanized checks for correctness, completeness, and

consistency, and to certify the obtained results. This in turn requires the adoption of a formal notation, which also ensures absence of ambiguity, thus preventing misinterpretation among people, participating to system requirements analysis, who often have quite heterogeneous cultural backgrounds. To facilitate communication, discussion, and mutual understanding, the formal notation must be flexible, expressive, and high level. It must be able to model in natural way real-world entities, basic notions such as events, actions, states (i.e., properties or values of system components, possibly having non null duration), continuity or finite variability, (non) determinism, and cause-effect relations. [3]

Re-engineering

There is a growing demand for software tools that can assist in designing, analyzing, and debugging embedded real-time applications. In the literature, various techniques based on real-time scheduling theory and formal methods have been proposed and many of them are implemented into software tools. Also, a number of commercial CASE tools have been developed and widely used. While most of these tools put an emphasis on the development aspect of embedded real-time systems, in practice, a great deal of effort is put into re-engineering of already developed systems. The re-engineering of an embedded system is defined as a development task of meeting newly imposed performance requirements after its hardware and software have been fully implemented.

In the industry, a large number of new lines of products are released merely as update of older designs. During product's re-engineering cycle, developers are often faced with tasks which involve intensive hand-tuning of embedded system designs. These tasks are often very difficult to carry out since product's developments are usually under very strict cost and performance constraints. However, it is fairly obvious that such a naïve approach will fail in practice due to the excessive price of the final products. Thus, it is inevitable for the engineers to pinpoint performance bottlenecks in the old design and carefully choose only those parts that can lead to about 25% performance improvement at the least cost. Such a task of performance re-engineering will get even more difficult if the original developers have been relocated to another project, or if the original systems were developed in an ad hoc manner. Worse still, there are very few tools to aid in performing such a re-engineering task, even though engineers are under tight deadline constraints for reduced time-to-market. Performance re-engineering involves analyzing a heterogeneous distributed multiprocessor hardware platform since an embedded real-time system often consists of multiple microcontrollers, ASIC (application specific integrated circuits) chips, and electro-mechanical components. In addition, performance re-engineering possesses very distinct and inherent characteristics: (1) software and firmware code of the underlying system has been developed and well-tested; and (2) task allocation and scheduling have been already completed. [4]

Validation

At the end of the development cycle it must be decided whether a given system is safe to deploy in the intended application area. If this application area is safety critical, i.e., a failure of the computer system can result in high financial loss or even a catastrophe where human lives are endangered then this decision is difficult. Many safety critical applications demand a level of dependability that cannot be established by state of the art testing technology. Some trends in the field of validation of high dependability real-time systems are:

Process versus Product

Since it is beyond the state of the art to validate by testing that a large real-time system is free of critical design errors, the validation emphasis has shifted from the analysis of the product to the analysis of the

development process of the product in the past few years.

Worst Case scenario

The time specifications at the architecture design level, identify the deadlines the component must meet under all specified operational conditions. During component design it must be demonstrated, that these deadline will never be missed. A necessary prerequisite for this temporal validation is knowledge about a tight upper bound of the worst case execution time of all time-critical process inside a component.

Simulation

Large real-time systems require a closed loop simulation in the laboratory to demonstrate that the system provides the intended services.

Formal Verification

A safety case is the accumulation of evidence from different sources that establishes the rational basis for the decision that a safety critical complete system is safe to deploy. The formal analysis of critical algorithms that are used in the system can form a convincing argument in the safety case.

[1]

Composing Modules with Synchronization And Real-Time Constraints Using Category Theory

Nowadays, complex real-time/embedded software systems are typically being composed out of reusable and mostly deployable components. This paper authors are aware of the paper presented by Varma and Sinha which presents a formal framework that utilizes the concepts of category theory to provide for a rigorous, consistent and traceable composition of modules with constraints.

The main contributions of the paper are to:

- Introduce the formal framework to facilitate the composition process.
- Define modules and their contracts for their interactions.
- Illustrate composition with constraints and its correctness using concepts of category theory.

Their paper gives an overview of component (module) composition utilizing concepts of category theory. [8]

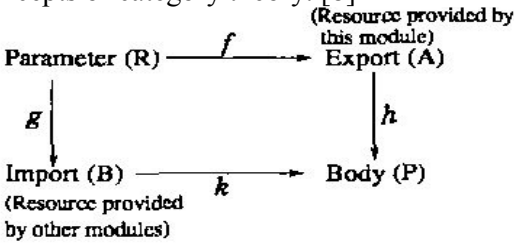


Figure 1: Module Interfaces

Module specifications are defined by utilizing the notion of push-out operation from category theory. Given specifications A and B, and a specification R describing syntactic and semantic requirements along with two morphisms f and g, the push-out operation gives specification R which contains A and B.

Composition of module specifications:

The composition scheme allows two modules to be interconnected via export and import interfaces. The push-out of the two modules is the resulting specification of the composed module.

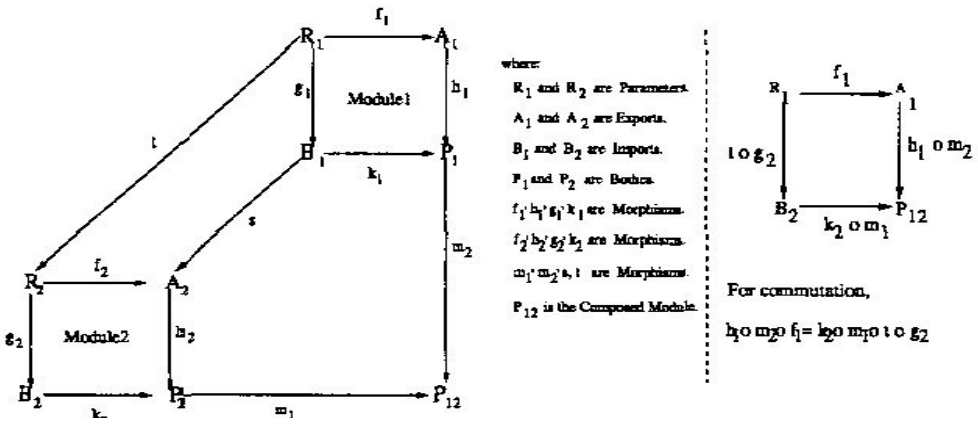


Figure 2: Composition of two modules

s

Figure 2 depicts the composition operation, where Module 1, M1 = (R1, A1, B1, P1) and Module 2 = (R2, A2, B2, P2). In Fig (a), Module 1 imports via specification B1 whatever Module 2 exports via specification A2. The compatibility of the parameters is governed by morphism t. In this case, the resulting composed module M12 is (R1, A1, B2, P12), where P12 is the push-out of P1 and P2 over B1. Furthermore, as the composed module commuted, i.e., its construction being proven correct, it can also be reused for subsequent composition.

Specifications with Constraints:

A module specification with constraints written as MC = (RC, AC, BC, P, f, k, g, h) consists of three specifications with constraints: (a) RC = (R, Cr), (b) AC = (A, Ca), (c) BC = (B, Ca), a specification without constraints P, and four morphisms f, k, g, h such that the basic part of M of MC given by M = (R, A, B, P, f, k, g, h) is a module specification without constraints).

Composition with Constraints:

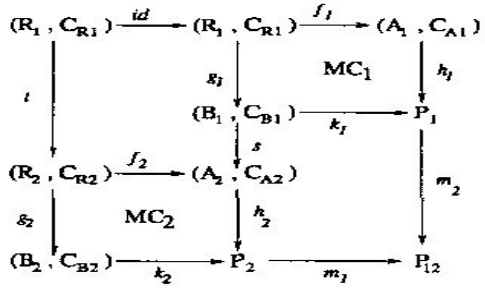


Figure 3: Composition of two modules with constraints

Given two module specifications with constraints MC1 and MC2 and an interface passing morphism v from MC1 to MC2 i.e., a pair v = (s, t) of specification morphism s: (B1, CB1) -> (A2, CA2) and t: (R1, CR1) -> (R2, CR2), the composition MC12 of MC1 and MC2 via v written as MC12 = {(R1, CR1), (A1, CA1), (B2, CB2), P12}.

Union with Constraints:

Given module specifications with constraints MCj for j = 0, 1, 2 and module morphisms f1: MC0 -> MC1 and f2: MC0 -> MC2, the weak union MC3 of MC1 and MC2 via MC0 is written as MC3 = MC1 + mcoMC2. Furthermore, PC3 = PC1 + pcoPC2, RC3 = RC1 + rcoRC2, AC3 = AC1 + acoAC2, and BC3=BC1+bcoBC2.

Proposed Framework

The main objective of proposed framework is to facilitate the composition of modules with constraints. The initial step is the identification of modules (components) based

on the working principles of the system. These components are then specified formally by defining sorts, operations and equations for the parameter, import and export interfaces of the component. A set of contracts or constraints for each of these components are defined along with their specification. Currently, contracts being defined include timing and synchronization constraints in the components. Other non-functional properties such as bandwidth and memory constraints can also easily be described as contracts. The composition of theses modules to result in a complete system is achieved via category theoretic operations. The final system is when verified for the correctness against a set of requirements prescribed for the system and the constraints resulting over the composition.

Concept of Contracts:

A software component can be defined as an independently deployable unit of composition with contractually specified interfaces. Internal contracts are constraints imposed on the stand-alone component. This generally deals with the initial values and constraints on the operations that can be performed by the component. External contracts are introduced as a result of inter-component interaction. The resulting constraints being imposed effect on the operation of the interacting components.

Contracts and Morphism Definitions:

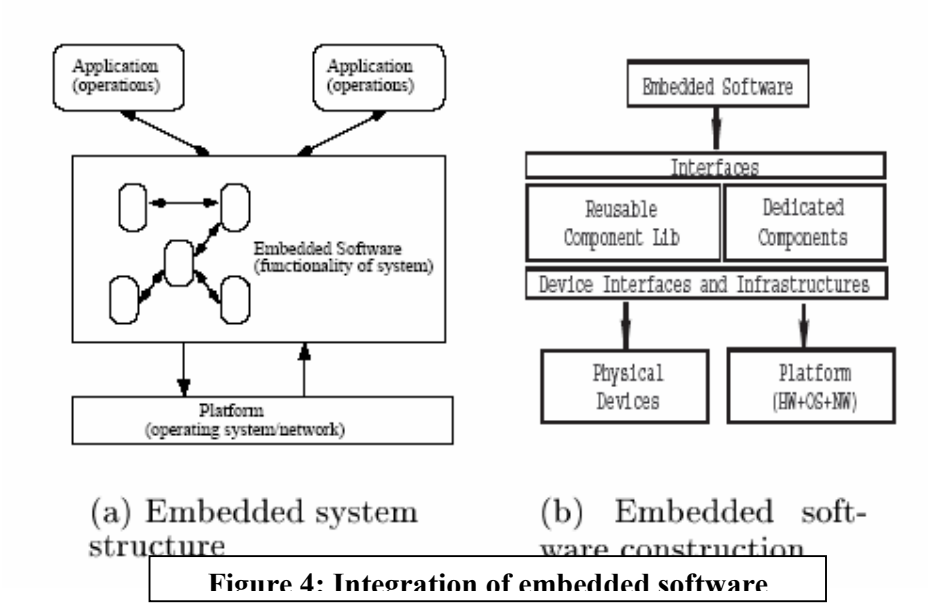
Morphisms define a rule in which two categories or components combine to form a composed category or components combine to form a composed category or a subsequently reusable component. Contracts play an important role in the morphism function definition. The morphism that combines two components is the functional implementation of the internal and external contracts that exist in each of the components. Thus, it can be summarized that morphisms are derived from the contracts that exist in each of the components.

Architecture for Embedded Software Integration using prototype Components

Behaviours of integrated software in the architecture proposed by Shige Wang and Kang G. Shin [12] is modelled as *Nested Finite State Machines* (NFSMs). The NFSM model supports compositional behaviour specifications. It further supports incremental and formal behaviour analysis. The behaviour correctness of such an integrated system can be verified using an approach similar to that in [10]. Furthermore, since a given behaviour can be implemented by different FSMs [11], different components may be selected for integration to meet different constraints while achieving the same behaviour. The behaviours specified in other models or languages can be converted to this model using translators. The integrated behaviours can then be specified in a Control Plan program for remote and runtime behaviour reconfiguration. This architecture also separates other non-functional constraints, especially timing and resource constraints, from functionality and behaviour integration so that these constraints can be analyzed and verified incrementally and as early as at design phase.

Component Structure

Components are pre-implemented software modules and treated as building blocks in integration. The integrated embedded software can be viewed as a collection of communicating reusable components. Figure 4 shows the embedded software constructed by integrating components.



(a) Embedded system structure

(b) Embedded software construction

Figure 4: Integration of embedded software

The component structure defines the required information for components to cooperate with others in a system. The software component is modeled as a set of external interfaces with registration and mapping mechanisms, communication ports, control logic driver and service protocols, as shown in Figure5.

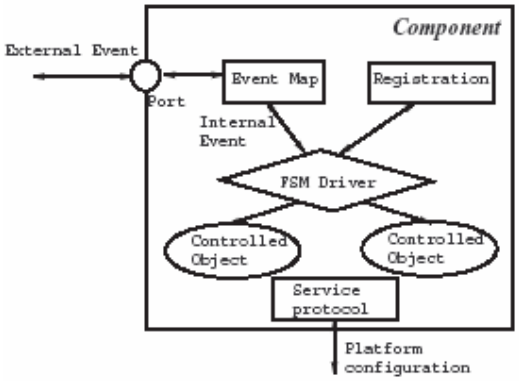


Figure 5: Reusable component structure

External interfaces:

External interfaces define the functionality of the component that can be invoked outside the component. In this model, external interfaces are represented as a set of acceptable events with designated parameters. A component with other forms of external interfaces, such as function calls, can be integrated into the system by mapping each of them to a unique event

Communication ports:

Communication ports are used to connect reusable components, i.e., they are physical interfaces of a component. Each reusable component can have one or more communication ports.

Finite State Machine driver:

The control logic driver, also called the FSM driver, is designed to separate function definitions from control logic specifications, and support control logic reconfiguration. The FSM driver can be viewed as an internal interface to access and modify the control logic, which is traditionally hard-coded in software implementation.

Service protocols:

Service protocols define the execution environment or infrastructures of a component. Example service protocols include scheduling policies, inter-process communication mechanisms and network protocols.

System Integration

Software integration includes component selection and binding, and control plan construction (both control logic and operation sequence). A runtime system can be generated by mapping the integrated software onto a platform.

Composition Model

The composition model defines how software can be integrated with given components. Since each reusable component is implemented with a set of external interfaces that uniquely define its functionality, components can be selected based on the match of their interfaces and design specifications. The integration of reusable components can be viewed as linking the components with their external interfaces. Reusable components in integrated software are organized hierarchically to support integration with different granularities, as illustrated in Figure6.

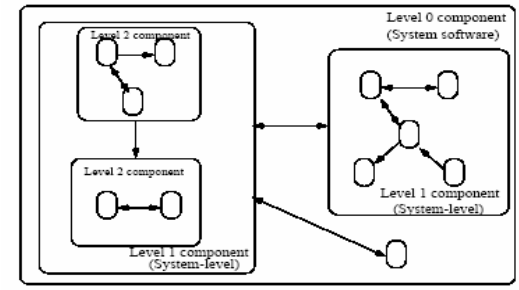


Figure 6: Hierarchical composition model

The behaviour of an integrated component can then be modelled as integration of its member component behaviours. The control logic and operation sequences of each component can be determined individually and specified in a Control Plan. The behaviour specifications can further be classified as device-dependent behaviours and device-independent behaviours. The device-independent behaviours depend only on the application level control logic, and can be reused for the same application with different devices. The device-dependent behaviours are dedicated to a device or a configuration, and can be reused for different applications with the same device.

With such a composition model, both components for low-level control such as algorithms and drivers and for high- level systems can be constructed and reused. However, additional overhead is introduced as the component level is increased, and may results in associated performance penalties due to excessive communications and code size.

Runtime System Construction

The integrated software obtained from the composition model cannot be executed directly on a platform since the composition model only deals with functionality. To obtain executable software, components have to be grouped into tasks, which are basic schedulable units in current operating systems. Each task needs to be assigned to a processor with proper scheduling parameters (e.g., scheduling policy and priority) determined by an appropriate real-time analysis. Also, communications among components should be mapped to the services supported by the platform configuration. After these pieces of information are obtained, the components can be mapped to the platform by customizing their service protocols. Figure 77 shows the mapping from functional integrated software to a runtime system with our architecture.

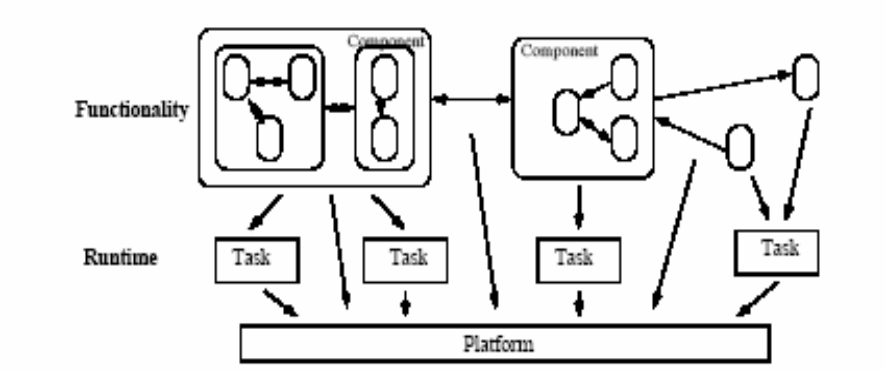


Figure 7: Runtime system generation from composition

Conclusion

This paper has put forth an initial effort in development of a formal framework for composition of modules that have synchronization and real-time constraints. Category-theoretic framework is discussed to assist realizing such compositions. One of the benefits of proposed framework is that it facilitates tracing of impacts or influences of a specific constraint imposed on a modules could have on other modules over an interaction.

In addition, a component-based architecture for embedded software integration is discussed above. This architecture defines components and a composition model as well as a behaviour model. A reusable component in the architecture is modelled with a set of events as external interfaces, communication ports for connections, a control logic driver (FSM driver) for separate behaviour specification and reconfiguration, and service protocols for executing environment adaptation. Such a well as behaviour reconfiguration. [12]

Lastly we discuss reusable component architecture for real-time systems. According to which these systems can be modelled with a set of events as external interfaces, communication ports for connections, a control logic driver for separate behaviour specification and reconfiguration, and service protocols for executing environment adaptation. The control logic of each component is specified in a state table separately from the component implementation, and can be reconfigured remotely and dynamically which also allows the verification to be done independently of implementation, and incrementally as the integration continues.

Recommendations

- The issue of reusable interface should form further research work in this area.
- The delivery method, and error detection in terms of quality assurance was also not treated because the operational specification in a real time distributed system with fail safe architecture was addressed and can form further research work in order to provide a good linking interface.

References

[1] Hermann Kopetz (2000). Software *Engineering* For Real-Time: A Roadmap. *Proceedings of The Conference On The Future Of Software Engineering*

[2] John A. Stankovic (1996) Strategic Directions in Real-Time and Embedded Systems. *ACM Computing Service, Vol. 28, No. 4.*

[3] Gargantini and Angelo Morzenti.(2001) Automated Deductive Requirements Analysis of Critical Systems. *ACM Transactions on Software Engineering and Methodology, Vol. 10, No. 3.*

[4] Minsoo Ryu, Jungkeun Park, Kimoon Kim, Yangmin Seo, and Seongsoo Hong(1999). Performance Re-engineering of Embedded Real-Time Systems. *ACM SIGPLAN Notices , Proceedings of the ACM SIGPLAN 1999 workshop on Languages, compilers, and tools for embedded systems, Volume 34 Issue 7.*

[5] Jan Richling, Matthias Werner, Louchka and Popova-Zeugmann (2002) "Automatic Composition of Timed Petri-net Specifications for a Real-Time Architecture"

[6] C. L. Liu and James W. Layland,(1979) "Scheduling algorithms for multiprogramming in a hard-real-time environment," *Journal of the ACM, vol. 20, no. 1.*

[7] Jan Richling (1999), "Komponierbare Echtzeitsysteme — Entwurfsmethodeund Architekturentwurf," Tech. Rep. Informatik Bericht 127, Institut f¨ur Informatik, Humboldt-Universit¨at, Berlin, Germany.

[8] Varma, N.and Sinha, P.(2003); Composing modules with synchronization and real-time constraints using category theory. Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on , Volume: 2 .

[9] Kopetz, H and Suri, N.(2003) Compositional design of RT systems: a conceptual basis for specification of linking interfaces. Object-Oriented Real-Time Distributed Computing, 2003. Sixth IEEE International Symposium .

[10] R. Alur and M. Yannakakis. (1998) *Model checking of hierarchical state machines*. In Proceedings of the 6th ACM Symposium on Foundations of Software Engineering, Lake Buena Vista, FL.

[11] T. Villa (1997). Synthesis of Finite State Machines: logic Optimization. Kluwer Academic Publishers.

[12] Shige Wang and Kang G. Shin (2000). An Architecture for Embedded Software Integration Using Reusable Components. In Proceedings of the 2000 international conference on Compilers, architecture, and synthesis for embedded systems.

On the Comparative Analysis of Determinant Factors on the use of Condom among Nigerian Youths.

Femi J. Ayoola[1], Lanre Faweya[2] and O.C. Oshodi[3]

[1,3] Department of Statistics, University of Ibadan, Nigeria.
2 Dept of Statistics, Ekiti State University, Ado-Ekiti
Corresponding Email: ayoolafemi@yahoo.com

Abstract

Condom use during sexual intercourse has been ascertained to be a good contraceptive method that reduces the spread of HIV/STDs. Youths which constitute a high proportion of Nigerians will be at risk of HIV/STDs if they miss the mark to use condom and more research should focus on how to encourage sexually active youth in protected sexually activities. This study utilized NARHS 2007 survey dataset. It focused on sample of males and females age 15-24 years living in regular households in rural and urban area in Nigeria. The dependent variables were lifetimes and current use of condom. Data was analysed using Chi-square and logistic regression (α=5.0%). Mean age of the respondent was 19.6±2.8, 25.1% are lifetime use of condom and current use of condom among those who had use condom in their lifetime was 72.2%.Youth's lifetime use of condom is statistically associated with all the background characteristics except marital status while current use of condom was found to be averse few of the selected variables such as Sex, Marital status, Number of sexual partners and alcohol intake.The odds of lifetime condom use were higher among older youths aged 20 – 24 years. Across the six geo-political zones; southern youth are more likely to use condom (OR = 7.2, CI = 4.5 – 11.6). Female are less likely to used condom. Condom use was found to increase as youth's education increases. Christians and multiple sexual partners are more likely. The youth with low perceived risk of HIV/AIDS are significantly more likely to use condom. Youth that takes Alcohol and drugs are more likely to use condom. In addition, the odds of females that are currently using condom decreases by 40% and the singles are 3times more likely for current use while youths with multiple sexual partners and those that also take alcohol are significantly more likely 3times more using condom.

Keywords: Condom, Sex, HIV/AIDS, Chi-square, Logistic regression

1.0 Introduction

The epidemic could increase at an exponential rate in Nigeria unless adequate national and regional responses are mounted to stem the spread of HIV/AIDS. According to Kaiser Family Foundation 2005, teens and young adults are in the centre of the epidemic because young people ages 15-24 account for approximately half of new adult HIV/AIDS infections that is the majority of those infected with HIV/AIDS has been affected with this virus before 25 years of age and 28% of the global total adults living with HIV/AIDS. Also United Nations Population Fund (2007) confirmed that young people are at the centre of the HIV/AIDS epidemic in terms of rates of infection, vulnerability and of the 1.5 billion young people worldwide, 11.8 million are estimated to be living with HIV. It is also reported that every day, between 5,000-6,000 young people (ages 15-24) contract HIV and that many of them still lack comprehensive and correct knowledge about to prevent the infection. that necessitate condom usage among the youths during sexual activities serve as the determinants of condom usage. The

It is generally known that youths sometimes adopted the use of condom during sexual intercourse and the factors

determinants of condom use among youths on compulsory paramilitary national service in Nigeria were documented to include influence of sexual partner, availability of condom, and self-efficacy of condom. (Sunmola A.M, Olley B.O, et al. 2007).Also, the major mode of HIV/AIDS transmission is through heterosexual intercourse in most part of the globe, including Nigeria. The estimated number of unwanted pregnancies and unsafe abortions in the country presents state can be outlining. The projection of unwanted pregnancies and unsafe abortion to maternal morbidity and mortality in the country is very high (WHO, 2005).

Globally, around half the people who acquire HIV become infected before they turn 25 years and they die before their 35th birthday (Worldwide HIV and AIDS Statistics Commentary, 2006). Thus, many people are sexually active and without adequate information to protect themselves. Therefore, this study will help to investigate the basic characteristics that influence the use of condom among Nigeria youths (15 to 24 years old). That is, to determine the prevalence of youths who had ever used condom, to determine the background characteristics that is likely to enhance the use of condom by the youths and to examine the sexual risk factors that may influence condom use among the youths.

2.0 Methods and Measurement

The study employed a secondary data used for National HIV/AIDS and Reproductive Health Survey (NARHS), 2007 with a (three level) multi-stage sampling targeted at selecting eligible persons in each sphere (states) with equal probabilities.Comprehensive report of the methodologies involved in data collection is available on the publication of the original data collector for details on the sampling procedures and validation of the study instruments.

In the original sample 11,521respondents were interviewed. Nevertheless, this study focused on youths aged 15-24 years, setting these inclusion criteria reduced the number of youth in the sample to 3,138. However, the number of youths who had ever had sexual intercourse whether vaginal, oral, anal or combination of any of them was found to be 787 and youths who currently use condom among those thatwere sexually active was 568.

Two dependent variables were used in this studyare; ever use of condom among the total study sample and currently use of condom among sexually active which is a subset of the studied sample. The variables was recoded into two categories; Condom = 1 and Otherwise = 0. The ever use of condom shows the level of condom use at any point in time in one lifetime while Current use of condom shows the present level of preventing sexually transmitted infections and unwanted pregnancies among youths in Nigeria.

3.0 Data analysis procedures

Data were analyses using Stata software version 12.0. The analysis began with Chi-square tests to establish associations in the selected variables. Afterwards Logistic regression was used for theoutcome variables lifetime user and current user to determine the strength of significant explanatory variables the youth.

Chi- Square test

The chi-square test is used to determine whether there is a significant difference between the expected frequencies and the observed frequencies in one or more categories. Is this difference between the expected and observed due to sampling error, or is it a *real* difference. Chi-Square Test requirements are: quantitative data, one or more categories, independent observations, adequate sample size (at least 10), Simple random sample, data in frequency form and all observations must be used.

The chi-Square formula:

$$\chi 2 = \frac{\sum_i^n (o-e)^2}{e} \qquad 3.1$$

Where ***o*** = Observed Frequency in each category
e= Expected Frequency in the corresponding category
df=degree of freedom (n-1)
χ2=is Chi Square

Logistic Regression

In the family of generalized linear models which contained models for categorical responses as well as standard models for continuous responses, the most important case is logistic regression, which is a linear model for the logit transformation of a binomial parameter.Binary logistic regression is a form of regression which is used when the dependent variable is dichotomy and the independent variables are of any type (i.e qualitative or quantitative) while Multinomial logistic regression is design to handle the case of more than two categories of dependent variable. When ranking of multiple classes of the dependent variable is put in place, then ordinal logistic regression is preferred to multinomial logistic regression. It should be noted that continuous variables cannot be used as dependents in logistic regression. So also there can be only one dependent variable in logit regression. Its predict a dependent variable on the basis of continuous and/or categorical independent variables and to determine the percent of variance in the dependent variable explained by the independents; to rank the relative importance of independents; to assess interaction effects; and to understand the impact of covariate control variables.

Logistic regression applies maximum likelihood estimation after transforming the dependent into logit variable (the natural log of the odds of the dependent occurring or not). In which case, logistic regression estimates the probability of a certain event occurring. And it calculates changes in the log odds of the independent but not changes in the dependent itself as ordinary least square does.

Logistic regression has many similarities to ordinary least square: logit coefficients correspond to β coefficients in the logistic regression equation, the standardized logit coefficient correspond to beta weights, and a R^2 statistic is available to summarize the strength of the relationship unlike ordinary least square. However, logistic regression does not assume linearity of relationship between the independent variables; the dependent does not require normally distributed variables, does not assume homoscedasticity and generally has less stringent requirement. In which case, logistic regression requires that observations are independent and that the logit of the independent variables is linearly related to dependent.

The logistic regression model is given as:

$$\log\left(\frac{\pi_i}{1-\pi_i}\right) = \sum_{k=0}^{K} \beta_k x_{ik} \text{ or}$$

$$log\left(\frac{\pi_i}{1-\pi_i}\right) = \alpha_0 + \beta_{1i}x_{1i} + \beta_{2i}x_{2i} + \beta_{3i}x_{3i} + \cdots + \beta_{ki}x_{ki}. 3.2$$

Where π_i is the outcome variable and i=1 if $\pi_i$is the proportion of youths who had used condom in their lifetime. Also, i=2 if $\pi_i$is the proportion of youth that still currently using condom in the sample studied. β's are the regression coefficients to be estimated, x's are the determinants such as age, location, zone, gender, marital status, education, religion, multiple partner, perceived risk alcohol intake and drug intake.

4.0 Results

The mean age and standard deviation of the respondents is 19.6±2.8. This data shows that a quarter (25.1%) of the respondent had ever used condom in their

lifetime while more than three-quarter (72.2%) of those that had ever used condom are still currently using condom. All the background characteristics were found to be significantly ($P<0.05$) associated with lifetime use of condom except marital status but marital status and gender was found to be significantly associated with current use of condom

.

Variables	Lifetime use of condom			Current Use of condom		
	Yes	χ^2-value	p-value	Yes	χ^2-value	p-value
Age		205.015	0.000		3.820	0.051
15-19	13.6(1506)			77.5(204)		
20-24	35.7(1632)			70.3(583)		
Location		8.894	0.003		0.276	0.600
Rural	27.8(1309)			73.1(364)		
Urban	23.1(1829)			71.4(423)		
Zone		198.249	0.000		7.468	0.188
North West	6.1(445)			55.6(27)		
North East	11.0(336)			59.5(37)		
North Central	25.9(591)			73.6(159)		
South West	32.3(679)			72.6(219)		
South East	23.1(463)			72.9(107)		
South South	38.1(624)			74.4(238)		
Sex		23.555	0.000		28.956	0.000
Male	28.3(1793)			78.5(508)		
Female	20.7(1345)			60.6(279)		
Marital Status		0.469	0.493		56.249	0.000
Single	24.8(596)			48.1(156)		
Married	26.2(2542)			78.1(631)		
Education		133.993	0.000		7.359	0.061
None	7.7(92.3)			70.0(20)		
Primary	17.3(433)			62.7(75)		
Secondary	25.6(2134)			71.6(546)		
Tertiary	46.8(312)			79.5(146)		
Religion		113.590	0.000		9.124	0.725
Islam	14.3(1160)			71.1(166)		
Christianity	31.4(1978)			72.2(621)		

Older youth aged 20-24 years (35.7%) were lifetime users of condom compared to younger youths aged 15-19 years (13.6%). Youths living in the rural location were slightly higher 27.81% than youths in the urban location (23.1%). The South South zone reported the highest lifetime use of condom (38.1%), followed by the South West (32%) while it was reported least in the North West zone of the country (6.1%). Also, males use of

Condom was found to higher than that of females (28.3% vs. 20.7%) while married youth used condom in lifetime than singles. Lifetime condom use by education reveals a trend; the higher the education, the more the use of condoms amongst these youth. The proportion of Christians using condom are about twice the proportion of Muslims making use of condoms (31% vs. 14.4%).

Furthermore, younger youth aged 15-19 years who are currently using condom (77.5%) is more than older youth aged 20-24 years(70.3%) who are lifetime use of condom were still currently using condom. The proportion of current use of condoms between rural and urban location were similar (73.1% vs. 71.3%). More so, current use of condom across the zone was highest in the South South region (74.3%) and least in the North West (55.6%). A higher percentage (78.5%) of the male

youths was more than females (60.6%) currently uses condom while married youths (78.1%) also have a higher use compared to unmarried youths (48.1%). Similarly, higher proportion of those that use condom currently were found to be more educated.

Table 2: Association of lifetime use and current use of condom selected behavioural characteristics

Variables	Lifetime use of condom			Current Use of condom		
	Yes	χ^2-value	p-value	Yes	χ^2-value	p-value
Multiple partner		63.612	0.000		24.125	0.000
No	44.1(1050)			71.1(463)		
Yes	69.8(314)			88.1(219)		
Perceived risk		69.166	0.000		5.510	0.064
High	36.3(91)			84.9(33)		
Low	32.5(1114)			74.9(362)		
No risk	19.5(1829)			69.2(357)		
Alcohol Intake		241.329	0.000		18.397	0.000
No	19.9(2650)			67.6(528)		
Yes	54.1(453)			82.5(245)		
Drugs Intake		17.177	0.000		1.206	0.272
Never use	24.7(3083)			71.8(760)		
Use drug	49.1(55)			81.5(27)		

In investigating the association between lifetime condom use and selected behavioural characteristics, youths with two or more partners representing 69.8% is significantly associated with lifetime use of condoms compared to youths that professed to have just one sexual partner (44.1%). Perceived risk of contracting HIV/AIDs is also associated with lifetime use of condoms among the youths while the proportion of perception is higher among the perceived high risk group. Again, both alcohol use and drug use is associated with lifetime use of condoms. The result shows that 54.1% of youths who takes alcohol and 49.1% who takes drugs were significantly higher than those who do not take any of these substances.

A similar scenario is observed among youths that currently use condom but there was no significant association for perceived risk of HIV/AIDS and drugs intake. Current use of condom was higher among youths with 2 or more sexual partners (88%) than those with only one sexual partner (71%). A majority (85%) of the youths rate their chances of getting HIV/AIDs as high and there was a decreasing pattern observed in these proportions as perceived risk decreases expressed by the youths that rate their chance of contracting HIV/AIDs. Also, there was a significant association between youths that currently use condom and alcohol intake (82.5%) and a similar proportion of 82% was observe among drugs users but not statistically significant.

5.0 Multivariate Analysis

In Table 3, older youths aged 20 – 24 years were 4times more likely to used condom compare to younger youths. Across the six geo-political zones; youth in the South-South are 7times more likely to use condom in their lifetime compare to youth in North west, follow by North west (put no of times here in bracket) and North Central youth who are six times more likely, also South East youth are about 4times more likely and lastly North East youth are 2times more likely to used condom in their lifetime. Female are less likely to used condom in their lifetime compare to male since the questions was centred on 'Have you ever used male condom', the probability that female will

use it is zero (β= -0.524 ε π_0). The higher the education level, the more youths are likely to use condom that is youth tends to lifetime use of condom as they go higher in their educational attainment compare to youth who do not have any academic background. It was also observed that the odds of youth who practice Christianityis 2times more compare to Muslim youth. Youth with multiple sexual partners are more like compare to youth with single partner. The odds of youth with high risk perception of contracting HIV/AIDS decreases by 25% though it is not statistically significant and youth with low risk perception of HIV/AIDs are significantly more likely to lifetime use of condom compare to youth that reported no perceived risk of HIV/AIDs. Youth that takes alcohol and drugs are more likely compare to those who do not.

However for current use of condom, the odds of female decreases by 40% compare to male since the questions was centred on 'Do you still use male condom in the last 12month', the probability that female will use it is zero (β= -0.516 ε π_0). An interesting thing is that marital status which has no significant association with the lifetime use of condom was significant in current use of condom. Youths who are not married are 3times more likely to current use condom compared to married youths. This shows that older youths who are married do not use condom to prevent pregnancy. Youths with multiple sexual partners are 3times more likely to be current condom users compare to youth with single partner and lastly those that take alcohol are significantly more likely compare to those who do not take at all.

Table 3: Logistic regression of lifetime and Current use of condom by selected characteristics

	Lifetime use of condom			Current Use of condom		
	P>|z|	**Exp(β)**	**95% CI for Exp(β)**	**P>|z|**	**Exp(β)**	**95% CI for Exp(β)**
Aged 20-24	0.000*	3.87318	(3.19319, 4.69798)			
Rural	0.053	0.83075	(0.68864, 1.00218)			
North East	0.032***	1.79576	(1.05087, 3.06886)			
North Central	0.000*	5.61596	(3.55281, 8.87723)			
South West	0.000*	6.04396	(3.83958, 9.51393)			
South East	0.000*	3.50062	(2.12067, 5.77851)			
South south	0.000*	7.20155	(4.45901, 11.6309)			
Female	0.000*	0.59206	(0.49233, 0.71200)	0.004**	0.59664	(0.42000, 0.84758)
Married				0.000*	3.11070	(2.09880, 4.61049)
Primary	0.155	1.50018	(0.85797, 2.62311)			
Secondary	0.009**	1.97598	(1.18676, 3.29004)			
Tertiary	0.000*	3.59880	(2.06699, 6.26579)			
Christianity	0.000*	1.70773	(1.33539, 2.18390)			
Multiple partner	0.000*	2.57761	(1.92723, 3.44747)	0.000*	2.73494	(1.72287, 4.34153)
Low risk	0.012***	1.35267	(1.06791, 1.71335)			
High risk	0.282	0.74360	(0.43347, 1.27561)			
Alcohol intake	0.000*	2.44218	(1.83085, 3.25763)	0.014***	1.71632	(1.11695, 2.63732)
Drugs intake	0.485	1.31142	(0.61123, 2.81370)			

**** Significant at 0.1%; **Significant at 1%; *** Significant at 5%***

6.0 Discussion

In spite of the high level on the awareness and knowledge of condom use around the globe, a greater proportion of youth still do not make use of it. According to Oyediran K.A., 2003, the effects of awareness of HIV/AIDS as a major determinant of condom use in Nigeria is the fact that the major motivating factor for condom use among monogamous married males was prevention of pregnancy and not

prevention of STIs. This draws an alarm on the needs to encourage youths through health talk, media shows, public seminar/workshop and other awareness forum on the danger, benefit and usefulness of condom to their health. Though condom was design primarily for family planning purpose but as AIDs epidemic is on the increase in recent times, condom use play a vital role in AIDs prevention campaigns and it has been reported in research work that condom can reduce the risk of contacting HIV/AIDS. Also United Nations Population Fund (2007) confirmed that young people are at the centre of the HIV/AIDS epidemic in terms of rates of infection, vulnerability and of the 1.5 billion young people worldwide, 11.8 million are estimated to be living with HIV/AIDS. It is also reported that every day between 5,000 to 6,000 young people (ages 15-24years) contract HIV and that many of them still lack comprehensive and correct knowledge on how to prevent the infection.

This research found that all the respondents (100.0%) aged 15 to 24years had heard of condom which agrees with Omorepie, G., study while one quarter of the youth had use condom in their lifetime and the three- quarter of those who had used condom are current user. About 60% of the youth reported they have no risk perception of HIV/AIDS, 37% indicated low risk perception and 3% with high risk perception. This was the main reason to examine if the use of condom depends on

the background (demographic) characteristics. . The chi square test of independence had reveals the association between lifetime use of condom and current use of condom with youth background characteristics and selected behavioural characteristics. Age group, location, geo-political zone, sex, Education level, religion, number of sexual partner, perceived risk of HIV/AIDs, alcoholic intake and drugs intake were found to be significantly associated with the lifetime use of condom while sex, marital status, number of sexual partner and alcoholic intake were found to be significantly associated with the current use of condom. Modelling the relationship of significant individual independent variables to the outcome variable-lifetime use and older youths aged 20 – 24 years were 4times more likely to used condom compare to younger youths. Across the six geo-political zones; youth in the South South are 7times more likely to use condom in their lifetime compare to youth in North west, follow by South west (6times) and North Central youth who are six times more likely, also South East youth are about 4times more likely and lastly North East youth are 2times more likely to used condom in their lifetime. Female are less likely to used condom in their lifetime compare to male since the questions was centred on 'Have you ever used male condom', the odds that female will use condom is less likely (0.6times). The higher the education level, the more youths are likely to use condom that is youth tends to lifetime use of condom as they go higher in their educational attainment compare to youth who do not have any academic background. It was also observed that the odds of youth who practice Christianity is 2times more compare to Muslim youth. Youth with multiple sexual partners are more like compare to youth with single partner. The odds of youth with high risk perception of contracting HIV/AIDS decreases by 25% though it is not statistically significant and youth with low risk perception of HIV/AIDs are significantly more likely to lifetime use of condom compare to youth that reported no perceived risk of HIV/AIDs. Youth that takes alcohol and drugs are more likely compare to those who do not. Thus, a logistic model was fit for the significant background and the selected behavioural characteristics.

However for current use of condom, the odds of female decreases by 40% compare

to male since the questions was centred on 'Do you still use male condom in the last 12month', the odds that female will use condom is still less likely (0.6times). An interesting thing is that marital status which has no significant association with the lifetime use of condom was significant in current use of condom. Youths who are not married are 3times more likely to current use condom compared to married youths; this can be traced back to a study in Zimbabwe that measures the change in HIV prevalence and sexual behaviour between 1998 and 2003. This shows that older youths who are married are not current user of condom supported by Meekers et al., 2003. Youths with multiple sexual partners are 3times more likely to be current condom users compare to youth with single partner and lastly those that take alcohol are significantly more likely compare to those who do not take at all.

7.0 Conclusion

Noticeably awareness and knowledge is not the hindrance but the low prevalence of lifetime use of condom can be traced to other numerous factors which the scope of this study cannot encompass. The background characteristics that are likely to enhance the use of condom for both lifetime use and current use differ. The lifetime use of condom was boost by all the demographic variables used except the marital status while current use of condom lean towards youth sex (gender), marital status, number of sexual partner and alcohol intake.

In order of eradicating HIV/AIDS, there is a need for sound education not watered one to the youths who are sexually active and Parents at large. Also, It will be a great phenomenon if Governments, Non-Governmental Organizations and other service providers place importance in dealing with the problem of HIV/ AIDS pandemic, especially sexually active youths in safe sex practice.

References

[1] Achebe, C.C., 1988. *Theories of Individual counselling: relevance to Nigerian situation.* Amherst. Massachusetts: Five-College Black Studies Press.

[2] Emenike K, 1997 Sexual Abstinence: A Viable Option for young Adolescent. In: DC Umeh (Ed.): *Confrontingthe AIDS Epidemic: Cross Cultural Perspective onHIV/AIDS Education.* Trenton NJ: Africa World Press, pp. 317-327.

[3] Heasrt N, Chen S. 2004 Condom Promotion for AIDS Prevention in the Developing World: Is it working? Studies in Family Planning 2004; 35(1): 39-47

[4] Imhonde HO, Azelama J, Aluede O 2005. HIV/AIDS: Sexual Risk Behaviour Associated with condom use: Assessing Attitude of Nigerian University undergraduate. *ICEPEC C D Journal*, XXC (3): 26-29.

[5] Olley B.O., 2001. Differences in Knowledge About HIV/ AIDS and Perceived Exposure to Risk Between Physician and Workers in Ibadan, Nigeria. *NigerianJournal of Psychology,* 2: 150-160.

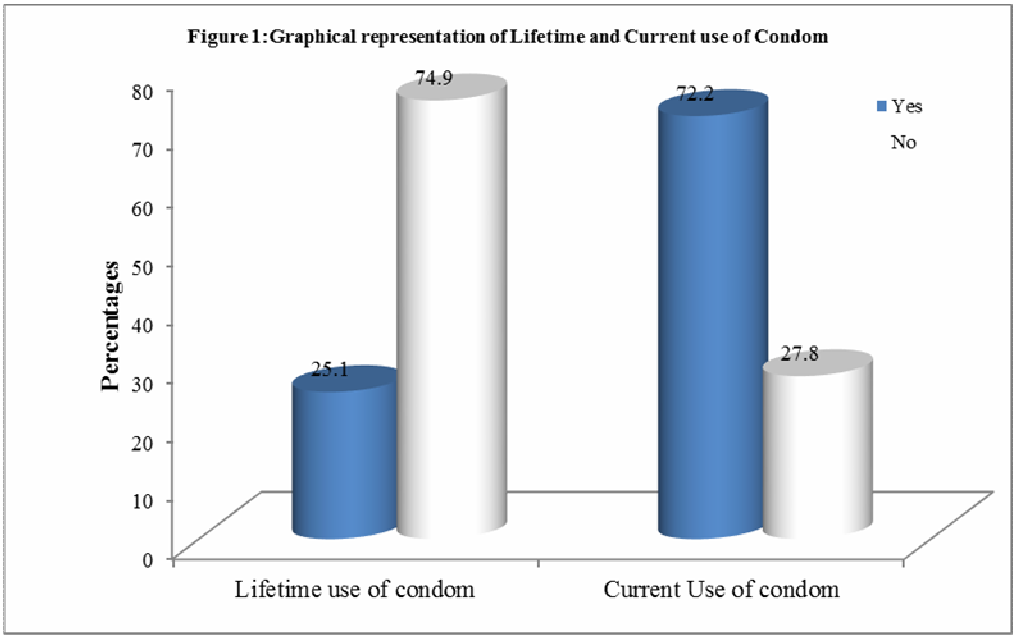
[6] Osho, A. and B.A. Olayinka, 1999.*Sexual practices conducive to HIV transmission in South West Nigeria*. Research on African HIV/AIDS epidemic Yaba: Lagos: St Luku Hospital and Maternity Ltd.

[7] Oyediran K.A., 2003 Determinants of condom use among monogamous men in Ondo State, Nigeria. J Health PopulNutr 2003; 21(4):358-66.

[8] Population Report 2001.*Youth and HIV/AIDS: Can We Avoid Catastrophe*. World Health Series, Geneva:World Health Organization Reports.

[9] Quadrel M.J., Fishholf B, Davis W 1993. Adolescent Morbidity.*American Psychologist,* 48(6): 28-42.
[10] Sunmola AM, Olley BO, et al.2007 Predictors of condom use among sexually active persons involved in compulsory national service in Ibadan, Nigeria. Health Educ Res 2007;22(4): 459-72.
[11] Tinuola F.R., 2006. Analysis of Some Key Sexual Bahaviour indicators among Adolescent in Ekiti South West Nigeria.*The Social Sciences,* 1(3): 171-177.
[12] World Health Organization (WHO). Maternal mortality in 2005: estimates developed by WHO, UNICEF, UNFPA and the World Bank. Geneva:WHO, 2007.
[13] Worldwide HIV and AIDS Statistics Commentary: http://www.avert.org/worlstatinfo.htm accessed 10 May 2006

APPENDIX



Th E P– Value Concept In Hypothesis Testing And Its Application On Mortality Rate Data

[1]Pwasong, A.D. and [2]M. Kembe A.

[*]**Department Of Mathematics, University Of Jos.** Davougus@Gmail.Com
[A]benue State University, Markurdi, Benue State

Abstract

This study is aimed at comparing the probability value (p – value) of various hypotheses tested with the specified level of significance α at 5% level. The study used data obtained from Hajiya Gambo Sawaba Government General Hospital Kofan Gaya, Zaria and other related examples to achieve this aim. The study involved the development and validation of the reasoning about p – values and statistical significance scale. The study finally recommends the use of p – value to take care of the probability of committing a type I error

Keywords: P – value, hypothesis, significance and infarct

1.0 Introduction

More often than not, experiments are carried out primarily to discover new facts or to test the result of previous findings. One of the most important tools in the analysis of experiment is hypothesis testing. [2], defined **test of hypotheses** or **test procedure** as a method for using sample data to decide between two competing claims (hypotheses) about a population characteristic. One hypothesis might be $\mu = 1000$ and the other $\mu \neq 1000$, or one might be $\pi = 0.01$ and the other $\pi < 0.01$. They further assert that, if it were possible to carry out a census of the entire population, we would know which of the two hypotheses is correct, but usually we must decide between them using information from samples.

According to [1] hypothesis testing is largely the product of Ronald Fisher, Jerzy Neyman, Karl Pearson and Egon Pearson. Fisher was an agricultural statistician who emphasized rigorous experimental design and methods to extract a result from few samples assuming Gaussian distributions. Neyman, who teamed with the younger brother Pearson, emphasized mathematical rigor and methods to obtain more results from many samples and a wider range of distributions.

The concept of p – values have been adopted widely in practice to avoid the imposition of the predefined level of significance that is always fixed at a specified level known as α – value. [8], defined the p – value as the probability of obtaining a value for the test statistic that is as extreme, or more extreme (taking account of the alternative hypothesis). They further explained that if the actual value of the statistics is too far from its expected value the test is deemed to be significant and the decision to reject H_0 in favour of H_1. If the actual value of the statistics is close to its expected value the test is deemed to be not significant and the decision is not to reject H_0. The set of values of the statistic that lead to rejection of H_0 is called the critical region or rejection region, and the set of values that do not lead to rejection of H_0 is called the acceptance region

.

The p - value being a probability can take any value between 0 and 1. Values closed to 0 indicate that the observed difference is unlikely to be due to chance, whereas a p - value close to 1 suggests there is no difference between groups other than that due to random variations.

More technically, a p – value of an experiment is a random variable defined over the sample of the experiment, such that, its distribution under the null hypothesis is uniform on the interval [0, 1]. Many p – values can be defined for the same experiment.

Frequent uses of a fixed level of significance have become a thing of concern in hypothesis testing. Looking into this, the use of p - value as a level of significance has become necessary. Many statisticians or experimenters are not aware of the use of p – values and tend to stick to a pre – selected level of significance which would not bring the true picture of whether a given level of significance is barely into a rejection region or far into the region. Hence, this paper is aimed at determining how to calculate p –values using appropriate test statistics and why p - values are preferable to other fixed level of significance, as well as the relationship between p – values and other level of significance.

Hypothesis testing is so important because it provides an objective frame work for making decisions using probabilistic methods, rather than relying on subjective impression. People can form different opinions by looking at data, but a hypothesis test provides a uniform decision making criterion that is consistent for all people. Hypothesis testing is also important and crucial in decision making. As part of statistical inference it is widely applied in various aspects of discipline such as: economics, business and science. P – values as an extension of hypothesis testing is very important as it provides the true value of α for which the data is significant. Once the p – value is known the decision maker can determine how significance the data are without the data analyst formally imposing a pre selected significance.

A review of the research literature from the field of statistics, statistical and mathematics education, psychology and educational psychology reveals difficulties or misconceptions students may have understanding probability and statistics. Researchers have examined how people's prior intuitions, heuristics, and biases may impact their reasoning about problems in probability, data analysis and descriptive statistics; for example, as in [3,5,6]. It was common in the past for researchers to classify results as statistically significant or non significant, based on whether the p – value was smaller than some pre – specified cut point, commonly 0.05. This practice is now becoming increasingly obsolete, and the use of exact p – values is much preferred. This is partly for practical reasons, because the increasing use of statistical software renders calculation of exact p – value simple as compared with the past when tabulated values were used.

The goal of this study is to develop an instrument for statistics education research that shows evidence of making inferences about student's inferential understanding. The study involved the development and validation of the reasoning about p – values and statistical significance scale.

2.0 Methodology

In another development,[7] asserts that the purpose of the p – value test is to facilitate statistics education research on students' conceptual understanding and misunderstanding of statistical inference and the effect of instructional approaches on the understanding. This section describes the method use to describe statistical significance and reasoning about p – values.

2.1 Data source

The data used for analysis in this paper was obtained from the secondary source, where the data is not originally collected by the investigator, but rather obtained

from published or unpublished sources. The data was obtained from a recognized government institution of the Federal Government of Nigeria. The institution is a hospital called " Hajiya Gambo Sawaba Government General Hospital" Kofan Gaya, Zaria. The data were from the medical record unit of the hospital.

2.2 The p – value

Statistical analysis is most useful when one is looking for difference that is small compare to experimental impression and biological variability. A p – value is a measure of how much evidence one has against the null hypothesis. The null hypothesis, traditionally represented by the symbol H_0 is true. The type of hypothesis tests (right tailed test, left tailed test or two tailed test) will determine what "more extreme" means. The p – value measures consistency by calculating the probability of observing the result from your sample of data or a sample with result more extreme, assuming the null hypothesis is true. The smaller the p – value, the greater the inconsistency of the null hypothesis. The general rule is that a small p – value is evidence against the null hypothesis while a large p – value means little or no evidence against the null hypothesis.

2.3 Statistical significance

The term significant is seductive, and it is easy to misinterpret it. A result is said to be statistically significant when the p-value is less than a present threshold value. It is easy to read into that word significant because the statistical use of the word has a meaning entirely distinct from its usual meaning. Just because a difference is statistically significant does not mean it is important or interesting. And a result that is not statistically significant (in the first experiment) may turn out to be very important.

If a result is statistically significant, there are two possible explanations:

(i) The populations are identical; so there is really no difference. You happened to randomly obtained larger values in one group and smaller values in the other, and the difference was large enough to generate a p - value less than the threshold you set. Finding a statistically significant result when the populations are identical is called making a type I error.

(ii) The populations really are different, so your conclusion is correct.

In writing up the result of a study, a distinction between scientific and statistical significance should be made, since the two terms do not necessarily coincide. The result of a study can be statistically significant but still not be scientifically important. This situation would occur if a small difference was found to be statistically significant because of a large sample size. Conversely, some statistically non-significant result can be scientifically important, encouraging researchers to perform large studies to confirm the direction of the findings and possibly reject H_0 with a larger sample size.

2.3.1 One vs two-tailed p-value method

When comparing two groups, you must distinguish between one and two-tailed p - values. Start with the null hypothesis that the two populations really are the same and that the observed differences between sample means is due to chance. The two-tailed p - value answers this question. Assuming the null hypothesis, what is the chance that randomly selected samples would have means as far apart as observed in this experiment with either group having the larger mean?

To interpret a one - tail p - value, you must predict which group would have the larger mean before collecting any data. The one - tail p - value answers these questions. Assuming the null hypothesis, what is the chance that randomly selected samples would have means as far apart as observed in this experiment with this specific group having the larger mean? A one-tail p - value is appropriate only when previous data, physical limitation or

common sense tell you that a difference, if any, can only go in one direction. The issue is not whether you expect a difference to exist that is what you are trying to find out with the experiment. The issue is whether you should interpret increases and decreases the same.

One should only choose a one-tail p-value when one believes the following:

(i) Before collecting any data, you can predict which group will have the lager mean (if the means are in fact different)

(ii) If the other group ends up with the larger mean, then you should be willing to attribute that difference to chance, no matter how large the difference.

It is usually best to use a two tailed p - values for these reasons:

(i) The relationship between p - values and confidence interval is clearer with two-tailed p - value.

(ii) Some tests compare three or more groups, which makes the concepts of tail inappropriate.

In other situations, you will want to make a decision based on a single comparison. In these situations, follow the steps of statistical hypothesis testing:

(i) Set a threshold p - value before you do the experiment. Ideally, you should set this value based on the relative consequences of missing a true difference or falsely finding a difference. In fact, the threshold value called (alpha) is traditionally almost always set to 0.05.

(ii) Define the null hypothesis. If you are comparing two means, the null hypothesis is that the two populations have the same means.

(iii) Do the .appropriate statistical test to compute the p - value.

(iv) Compare the p - value to the present threshold value. If the p - value is less than the threshold, state that you "reject the null hypothesis" and that the difference is "statistically significant". If the p - value is greater than the threshold value, state that "do not reject the null hypothesis" the difference is not "statistically significant."

2.3.2 P- value under single value (one -tailed test)

A test of any statistical hypothesis, where the alternative hypothesis is expressed by means of a less than symbol (<) or greater than symbol (>) is called a one tailed test, since the entire critical region lies in one tail of the distribution of the test statistic. The symbols < or > point to the direction of the critical region. The steps for testing a hypothesis about a mean of a population with known variance against one sided alternative hypothesis may be summarized as follows:

(i) Ho: $\mu = \mu_0$

(ii) H_1: alternative is either $\mu < \mu_0$ or $\mu > \mu_0$

(iii) Choose a level of significance equal to α

(iv) Critical region $Z < -Z_\alpha$ for the alternative $\mu < \mu_0$ or $Z > Z_\alpha$ for the alternative $\mu < \mu_0$

where Z has a standard normal distribution. Compute $\bar{x}$ from a random sample of size n, and then find $Z = \dfrac{\bar{x} - \mu_0}{\dfrac{\sigma}{\sqrt{n}}}$

(v) Conclusion: Reject H_0 if Z falls in the critical region otherwise accepts H_0.

We can solve for p as a function of Z

by: $p = \phi(z_p) = \phi(z) = \phi\left[\dfrac{\bar{x} - \mu_0}{\sigma/\sqrt{}}\right]$

Example: A topic of recent clinical interest is the probability of using drugs to reduce infarct size in patients who have had a myocardial infarction within the past 24 hours. Suppose we know that in untreated patients the mean infarct size is 25 with a standard deviation of 10. Furthermore, in 8 patients treated with the drug, the mean infarct size is 16. Is the drug effective in reducing infarct size? (Use $\alpha = 0.05$).

Solution: The hypotheses are:
Ho: $\mu = 25$ versus H_1: $\mu<25$, $\sigma=10$ and n = 8
The p-value is computed using

Hence, p = 0.005 < 0.05. Thus H_0 is rejected and we conclude that the drug reduces infarct size.

The importance of p-value is that it tells us exactly how significant the results are without performing repeated significance tests at different levels. In the above example the p-value is equal to 0.005 and thus the results are highly significant, which is known under the null hypothesis $\bar{x} \sim N(\mu_0, \sigma^2/n)$ .Hence the probability of obtaining a sample that is no larger than $\bar{x}$ under the null hypothesis is: $\phi\left[\frac{x-\mu_0}{\sigma/\sqrt{n}}\right] = \phi(z)$ = p-value
These are extracts from [3].

2.3.3 P - value under single value (two-tailed test)

A test of any statistical hypothesis where the alternative is written with a non-equal sign ($\neq$) is called a two-tailed test, since the critical region is split into two equal parts, one in each tail of the distribution of the test statistic.
The null hypothesis, H_0 will always be stated using the equality sign so as to specify a single value. In this way the probability of committing a type 1 error can be controlled. The steps for testing a hypothesis about a mean of a population with known variance ∂^2 against two-sided alternative hypothesis may be summarized as follows:

(i) Ho: $\mu = \mu_0$
(iii) H_1: $\mu \neq \mu_0$
(iv) Choose a level of significance equal to α
(v) Critical region $Z < -Z_\alpha/2$ and $Z > Z_\alpha/2$ for the alternative $\mu \neq \mu_0$ where Z has a standard normal distribution. Compute x

$$p = \phi(Z_p) = \phi_{(z)} = \left[\frac{16-25}{10/\sqrt{8}}\right] = \phi(-2.55) = 1 - \phi(2.55) = 1 -]$$
$$= 0.9945 \approx 0.005$$

from a random sample of size n and then

$$find\ Z = \frac{x-\mu_0}{\sigma/\sqrt{n}}$$

(vi) **Conclusion**: reject H_0 if Z falls in the critical region otherwise accept H_0.

These are extracts from [7].

2.3.4 Determining the p - value for one sample Z test

To determine the p - value for the one-sample Z test for the mean of a normal distribution with known variance (two – alternatives) is given

by: $p = \begin{pmatrix} 2\phi(z) & if & z \leq 0 \\ 2(1-\phi(z)) & if & z > 0 \end{pmatrix}$

Thus, in words, if $Z \leq 0$, then p = 2 times the area under an N (0, 1) distribution to the left of Z; if Z > 0, then p = 2 times the area under an N (0,1) distribution to the right of Z. Using the above example we have:

H_0: $\mu = 25$ versus H_1: $\mu \neq 25$, $\sigma=10$
The p - value is computed using

p = 2 x ϕ(-2.55)
= 2 x [1 - ϕ(2.55)]
= 2 x (1 - 0.9945)
= 2 x 0.005 = 0.01
p = 0.01 < 0.05

Therefore we reject H_0 and conclude that the drug reduce infarct size.

2.3.4 P-value between two values (one-tailed test)

The steps for calculating p - value between two values with one-sided alternative is the same as the one considered in 2.3.3 above, the only difference is that the levels of significance

alpha (α) are in two different forms. If we decide to use two different levels of α at 0.05 and 0.01 respectively, we may want to determine whether H_0 is rejected at both levels of significant or accepted in one of the levels and rejected in the other. From our previous example we know that the p - value, using one sided alternative is 0.005. If we compare this value with the two levels of α i.e. 0.05 and 0.01, we will notice that the p - value which is 0.005 is so small compare to these two values. So we reject H_0 and conclude that the result is highly significant.

2.3.5 P-value between two values (Two-tailed test)

To calculate p – value between two values with two-sided alternative requires the following steps:

(i) Set H_0: $\mu = \mu_0$

(ii) Set H_1 :$\mu \neq \mu_0$

(iii) Choose a level of significance α. In this case α is chosen at two levels (0.01 and 0.05)

(iv) Critical region $Z < -Z_{\alpha/2}$ and $Z > Z_{\alpha/2}$ for the alternative where Z has a standard normal distribution. Compute X from a random sample of size n, and then find Z

$$= \frac{x - \mu_0}{\sigma / \sqrt{n}}$$

We can calculate p - value in terms of Z i.e. p = ϕ(Z). Since it is two-sided alternative we have:

$$P = \begin{pmatrix} 2\,\phi_{(z)}, & ifz \leq o \\ 2\,(1 - \phi_{(z)}), & ifz \geq 0 \end{pmatrix}$$

Using our previous example we have

$$p = \phi(Z_p) = \phi_{(z)} = \left[\frac{16 - 25}{10/\sqrt{8}}\right] = \phi(-2.55)$$

Therefore, for two-sided alternative we have:

2 (1 – ϕ(2.55)) = 2 (1 - 0.9945) = 2 (0.005) = 0.01. Therefore p = 0.01.

Conclusion: Since 0.01 < P < 0.05, we reject H_0 and conclude that the result is statistically significant (i.e. the drug may reduce the infarct size).

3.0 Data Presentation

The data in table 1 and 2 are part of the secondary data collected from the Hajiya Gambo Sawaba Government General Hospital Kofan-Gayan, Zaria, Kaduna State. The data were subjected to analysis using Predictive Analytic Software (PASW), with a view to calculating the p - value for all the hypotheses under consideration

.

Table 1: Mortality rate by sex distribution of Hajiya Gambo Sawaba Government General Hospital, Zaria in 1999.

Male	8	3	12	11	6	8	10	12	6	17	2	8	9	9	8	2
Female	10	14	6	3	9	6	6	3	4	20	2	4	6	7	4	8

Table 2: Mortality rate by age\ sex distribution of Hajiya Gambo Sawaba Government General Hospital, Zaria

Year	Age					
	0 – 14		15 – 64		65 and above	
Sex	M	F	M	F	M	F
1995	50	34	66	36	15	42
1996	28	13	84	28	26	38
1997	12	20	92	12	17	32
1998	15	21	80	32	42	58
1999	22	29	90	47	24	35
2000	33	24	38	92	30	12
2001	22	24	46	18	32	25
2002	20	32	58	24	22	50
2003	28	39	72	49	40	29
2004	44	31	124	49	42	54
2005	21	28	40	98	36	28
2006	30	40	45	80	22	39

3.1 Analysis and Results.

The data was analyzed using the Predictive Analytic Software (PASW) and tables 3(a), 3(b), 4 and 5 revealed the results obtained. The level of significance is 0.05 and the various hypotheses to be tested are listed below:

(i) H_0: There is no significant difference between male and female with respect to mortality rate.

(ii) H_1: There is significant difference between male and female with respect to mortality rate.

(iii) H_0: There is no significant difference between sex and age group with respect to mortality rate.

(iv) H_1: There is significant difference between sex and age group with respect to mortality rate.

.

Table 3(a): t – test for sex with respect to mortality rate (Group Statistics)

	Sex	N	Mean	Std. Deviation	Std. Error Mean
Mortality rate	Male	16	8.1875	3.93647	0.9841
	Female	16	7.000	4.6188	1.1547

Table 3(b): Independent sample test

Mortality Rate		Levene's test forEquality of variances		t – test for equality of means						
		F	Sig.	t	df	Sig.(2-tailed)	Mean difference	Std.error difference	95% Confidence	
	Equal variances assumed	0.162	0.691	0.783	30	0.44	1.1875	1.51718	-1.9	4.29
	Equal variances not assumed			0.783	29.265	0.44	1.1875	1.51718	-1.9	4.29

3.2 Interpretation

In comparing mortality rate between male and female in Sawaba Government General Hospital, Zaria in 1999. The result above clearly portrayed there is no significant difference between male and female with respect to mortality rate. At 5% significance level, the p-value which is 0.44 is greater than 0.05. Hence we conclude by accepting the null hypothesis that there is no significant difference existing between male and female mortality rate. For the chi-square test, the results in tables 4 and 5 were obtained

.

Table 4: Sex and age group cross tabulation

Crosstab

			Age			Total
			0 -14	15 - 64	65 - above	
Sex	M	Count	325	836	348	1509
		Expected Count	349.3	741.5	418.1	1509
	F	Count	335	565	442	1342
		Expected Count	310.7	859.5	371.9	1342
Total		Count	660	1401	790	2851
		Expected Count	660	1401	790	2851

Table5: Chi-Square Test

	Value	df	Asymp. Sig(2-sided)
Pearson Chi-Square	54.160[a]	2	0.000
Likelihood Ratio	54.327	2	0.000
Linear-by-Linear Association	5.83	1	0.016
No of Valid Cases	2851		

[a] cells (0%) have expected count less than 5. The minimum expected count

From the table above we can say that the difference between sex and age group with respect to mortality rate is highly significant. Using p - value approach the null hypothesis is rejected since p - value at 0.000 is less than 0.05 level of significance. We therefore, conclude that the mortality rate does not depend on age and sex.

4.0 Conclusion and Recommendation

From the above results, it is seen that the conclusion reached using p - value at α (alpha) level of testing is more accurate and more reliable that those reached using other criteria.

The use of p-value did not only show the significant difference but also revealed how significant the observed difference is in statistical point of view. We can deduce

from the p - value whether the observed difference is far into the critical regions or merely into the regions and with this information, we can decide whether the data should be adjusted to meet up with the desired accuracy or be thrown aside completely.

Finally p - value do not only offer experimenters or investigators varieties of choices, but also eliminate the fear of imposition of pre-set level of significance that always result in reaching partial or inadequate conclusion whenever an experiment or trial is conducted. The main goal in this research work is to compare the probability value (p-value) of various hypotheses tested with the specified level of significance α (alpha) at 5% level with a view to determining whether the null hypothesis should be rejected or not.

One of the most important advantages of p-value in hypothesis testing is its ability to eliminate the fear of doubt as regarding the validity of conclusions being drawn from the result of an experiment. Since performing experiments cost money, time, energy and resources. Utmost caution has to be exercised before drawing conclusions. Unfortunately, many experimenters or investigators are not aware of the use of p - values and for this reason, it is recommended that p - values should always be used in hypothesis testing rather than the pre-set level of significance that we are conversant with.

Also since a p-value conveys much information about the weight of evidence against the null hypothesis and knowing fully from the fact that rejecting a true null hypothesis H_0 implies probability of committing type I error, therefore, recommends the use of p - value to take care of this error.

.

References

[1] Cobb, G. (1992). Teaching statistics. In L.A. Steen (Ed:), *Heading the case for change : Suggestions for curricular action (pp. 3 – 43).*Wasshington, D.C: the Mathematical Association of America.

[2] Devore, J., & Peck, R. (2006). *Statistics: The exploration and analysis of data (5th ed:),* Belmont; CA: Brooks/ Cole – Thomson Learning.

[3] Garfield, J., & Ahlgren, A. (1988). Difficulties in learning basic concepts in probability and statistics: *Implications for research. Journal for Research in Mathematics Education 19(1),* 44 – 63.

[4] Huberty, C.J. (1993). Historical origins of statistical testing practices: *The treatment of Fisher versus Neyman – Pearson view in textbooks. Journal of Experimental Education, 61(4),* 317 – 333.

[5] Kahneman, D., & Tversky, A. (1982). Subjective probability: A judgement of representativeness. In D. Kahneman, P. Slovic & A. Tversky (Eds.), *judgement under uncertainty: Heuristics and biases (pp. 32 – 47)*: Cambridge: Cambridge University Press

[6] Konold, C. (1995). Issues in assessing conceptual understanding in probability and statistics. *Journal of Statistics Education, 3(1). Retrieved march 20, 2007,* from http://www.amstat.org/publications/jse/v3n1/konold.htm/

[7] Nickerson, R.S. (2000). Null hypothesis significance testing: A review of an old and

continuing controversy. *Psychological methods, 5(2), 241* - 301

[8] Saldanha, L.A., & Thompson, P.W. (2006). Investigating statistical unusualness in the context of a resampling activity: Students exploring connections between sampling distribution and statistical inference. In A. Rossman & B. Chance (Eds). *Working cooperatively in statistics education: Proceedings of the Seventh International Conference on Teaching Statistics. Retrieved March 20, 2007, from http://www.stat.auckland.ac.nz/~iase/publications/17/6A3-SALD.pdf*

Examination of Reviews-Outcomes of Community Water Fluoridation in Dental Caries Prevention

[1]Oluchi A. Olofin, [2] Comfort N. Agu & [3]Nkechi O. Ohadoma

[1,3]Department of Dental Therapy, Federal School of Dental Technology & Therapy, Trans-Ekulu, PMB 01473, Enugu, Nigeria
[2]Department of Human Kinetics and Health Education, Enugu State College of Education (Technical) PMB 01793, Enugu, Nigeria
[1]Cell: +2348034711552; Email: oluchiolofin@gmail.com [2]Cell: +2347065241311; Email: comfortagu@gmail.com
[3]Cell: +2348035902119; Email: angelohadoma@yahoo.com

Abstract

The purpose of this paper is to examine the different reviews of the outcomes of fluoridation of community water in the prevention of dental caries in Cochrane library. The earlier articles within the period, 2010 and 2013, were introduced in this study. As dental caries has remained a challenge in public health where the quantity of fluoride in water is low (lower than the recommendation of World Health Organization 1 part per million (ppm)). The positive effects of fluoridation of community water in the prevention of dental caries are recognized in a widely manner, especially in the consideration of children. In some selected reviews, it was discovered that fluoride is effective in the prevention of dental caries in people whose ages are more than 20 years. There is a relationship between the concentration of water fluoridation of quantity higher than 1 ppm and the incidence of dental fluorosis. It was also observed that there is no relationship between fluoridation and cancer or bone fracture, or any other effects. As fluoridation of water is of immense benefit to a community with higher population, the authors and researchers also acknowledged and recommended other sources of fluoride such as milk, salts, and toothpaste, for prevention.

Keywords: fluoride, dental caries, cancer, water fluoridation, community water, oral diseases.

1.0 Background of the study

The main pathway of the human body system through drinking, eating, and speaking is the mouth. According to [7], an integral aspect of the total well-being of any individual is the oral health. The moment the oral health of a person is good, such individual will effectively communicate and consume any type of food, and able to live a quality lifestyle, social confidence and self-esteem [17]. Watt further expatiated that when oral diseases such as periodontal diseases, dental caries, dental erosion, and oral cancers, could hinder the individual from a happy lifestyle. These diseases have affected a notable portion of the world's population, in terms of mortality and morbidity. There is a high prevalence of oral diseases; hence the negative impact on the society is noticeable. Some of impacts of these diseases include discomfort, pain, sleeplessness, inability to eat effectively and absenteeism from work or school [17].

There have been remarkable effects on nutrition in developing countries due to changes in political, economic and social aspects, thus shifting the people from consuming local and traditional foods to diets of Western countries [15]. According to [14], one of the major health challenges in almost all industrialized countries is dental caries. According to [15], the number of children in school is within the range of 60 and 90%, and high proportion of adults is involved. Petersen & Lennon

further stated that dental caries is caused by high rate of sugar consumption and lack of adequate exposure to fluoride.

The disease dental caries is preventable [14], and this can be controlled when there is synergy between health professionals and individuals by adopting methods that will help in the reduction of sugar consumption and the creation of awareness on the benefits of fluorides. Fluoridation of community water is aimed at reaching the larger population. According to [1], more than 144 million people have access to drinking water that belongs to the community. A study titled "community effectiveness of public water fluoridation in reducing children's dental disease" was conducted by [2]. The study compared children's decay experience and prevalence between areas with and without water fluoridation in Australia. The outcome of the study was that all the categories of the children had higher cases of dental caries.

Fluorine has been used in the prevention of cavities when observed with people that grew up drinking water that contained fluoride, and as such had minimal cases of cavities [7]. Studies on effect of fluoride on oral health commenced over 100 years ago, but 50 years earlier, the studies focused on the relationship between water-borne fluoride, dental caries, and fluorosis [15]. Sequel to this was the focus on the evaluation and development of fluoride rinses, toothpaste, milk, and salt [15]. Notable articles have been printed on the outcome-effects of the use of fluoride on humans, and an inquiry into the database has shown proofs on the subject. The UK University of York Centre for Review and Dissemination conducted some systemic reviews on water fluoridation in the specialized areas of fluoride ingestion, fluoride toothpastes and fluoride rinses using the Cochrane Collaboration Oral Health Group. The summary is as follows:

1) There is a reduction of the frequency of dental caries through the use of water fluoridation by 15% (2.2DMFT).
2) Toothpastes with fluoride and mouthwash rinses cause a reduction of DMFS 3-year
increment by 24 to 26%.
3) There is no reliable evidence of the adverse effect of water fluoridation.
4) There is a level of concentration where there is a relationship between water
fluoridation and dental fluorosis.
5) There was no evidence of a research into the adverse effect of the use of fluoride
toothpaste and mouth wash rinses.

The benefits of water fluoridation are acceptable in developing countries as explained by [9]. This complements the review of the success of water fluoridation in United States of America because there are other methods of the provision of fluoride and the availability of the products that contain fluoride which reduces the prevalence of dental caries.

2.0 Objective

The objective of this paper is the evaluation of the effectiveness of fluoridation of community water in the reduction of dental caries disease. In achieving this, review of related literatures in Cochrane review will be done.

2.1 Selection Criteria

1) ***Types of Studies***: The studies conducted by using the non-randomized control trials, case or
cohort control studies were well-researched. The report was well written in the language of communication, English language.
2) ***Types Participants***: The participants were school children that profited from the water
fluoridation intervention program.
3) ***Types of Intervention***: these are distinct programs on water fluoridation targeted at
the prevention of dental caries executed at the community. All the participating children were visited in their homes, schools, and

through the health workers in their various communities.

4) ***Types of Outcome Measures***: the children that attended the screening program of the oral health judged the outcome of the status of the oral health.

2.3 Search Strategy for Identification of Studies

In the course of this study, relevant literatures on fluoridation of water and prevention of dental caries were reviewed using Cochrane Database of Systemic Review, PUBMED, MEDLINE, CINAHL and Google Scholar. Though some relevant materials were retrieved form Cochrane Library, but most of the works cited were from other sources.

3.0 Methods of Review

The articles selected were based on the key terms related to the seminar topic. A related article was retrieved from the Cochrane Library, but other materials received through Google Scholar were relevant to the study. All the materials are from the search criteria, "water fluoridation", and they were within the period 2010 and 2013.Quantitative approach methodology was adopted by these studies.

3.1 Description of Studies

From the ten articles found from the database and through Google Scholar, all are related to water fluoridation. These research papers discussed the prevention of dental caries using fluoridation. The participants in all the studies were children of different age categories. Results from other relevant papers were also presented by most of the articles reviewed. In these articles, some of the authors stated to have reviewed similar studies of over 20 articles.

3.2 Methodological Quality of Included Studies

The studies were well-conducted and utilized standard methodology. All these studies had abstract except one that is a protocol for review. Furthermore, each of the articles had objectives of the study, background, method, results and discussion section, conclusion, and the references.

4.0 Results

In the study conducted by [2], the result showed that Children from every age group had greater caries prevalence and more caries experience in areas with negligible fluoride concentrations in the water (<0.3 parts per million [ppm]) than in optimally fluoridated areas (> or = 0.7 ppm). Controlling for child age, residential location, and SES, deciduous and permanent caries experience was 28.7% and 31.6% higher, respectively, in low-fluoride areas compared with optimally fluoridated areas. The odds ratios for higher caries prevalence in areas with negligible fluoride compared with optimal fluoride were 1.34 (95% confidence interval [CI] 1.29, 1.39) and 1.24 (95% CI 1.21, 1.28) in the deciduous and permanent dentitions, respectively. The study conducted by [3] revealed that children who brushed their teeth less often and were older, male, of low SES, from rural or remote areas consumed significantly more SSBs. Caries was significantly associated with greater SSB consumption after controlling for potential confounders. Finally, greater exposure to fluoridated water significantly reduced the association between children's SSB consumption and dental caries.

According to the result presented by [5], the review describes the main sources of fluoride intake that have been identified: fluoridated drinking water, fluoride toothpaste, dietary fluoride supplements and infant formulas. Recommendations on how to avoid excessive fluoride intake from these sources are also given. The result, according to [6] showed that no study evaluated effects of screening by primary care providers on clinical outcomes. One good-quality cohort study

found pediatrician examination associated with a sensitivity of 0.76 for identifying a child with cavities. No new trials evaluated oral fluoride supplementation. Three new randomized trials were consistent with previous studies in finding fluoride varnish more effective than no varnish (reduction in caries increment 18% to 59%). Three trials of xylitol were inconclusive regarding effects on caries. New observational studies were consistent with previous evidence showing an association between early childhood fluoride use and enamel fluorosis. Evidence on the accuracy of risk prediction instruments in primary care settings is not available.

[8] commented that the prevalence of fluorosis (TFI ≥1) in communities with 0.70 and 1.50 ppm water fluoride was 39.4 and 60.5% ($p = 0.014$), respectively, while the prevalence of more severe forms (TFI ≥4) was 7.9 and 25.5% ($p < 0.001$), respectively. The mean D3MFT was 0.49 (±1.01) in the 0.70 ppm community and 0.61 (±1.47) in the 1.50 ppm community ($p = 0.349$). A logistic regression model for caries (D3 >1) showed that higher fluorosis categories (TFI 5-6 OR = 6.81, $p = 0.001$) were associated with higher caries experience, adjusted by age, number of teeth present, tooth brushing frequency, bottled water use, and natural water fluoride concentration. [10] found that one hundred and ninety children (mean age: 36.3 ± 6.9 months) were recruited from six community medical clinics. Ninety-two children (48.4%) were caries active. The mean d(123) t and d(123) s scores were 2.2 ± 3.3 and 3.0 ± 5.6, respectively. Higher plaque scores were significantly ($P < 0.0005$) associated with all measures of decay (presence of decay, dt, ds).

The risk factors for severity of decay (i.e., dt and ds) include child's age, breastfeeding duration, and parents' ability to withhold cariogenic snacks from their child. According to [11], the objectives of the study are two-fold: to evaluate the effects of water fluoridation (artificial or natural) for the prevention of dental caries; and to evaluate the effects of water fluoridation (artificial or natural) on dental fluorosis. In measuring the percentage prevalence of fluorosis, all children with fluorosis according to the index used will be classified as 'fluorosed' as opposed to normal. As measured by the common epidemiologic indices for dental fluorosis [18], children with a DDE, TSIF, TFI score greater than zero or Dean's classification of 'questionable' or higher will be classified as fluorosed. If the other indices are used, the percentage prevalence of fluorosis as reported by the original investigators using other methods (e.g. photographic method or other index) will be considered and adopted. Any fluorosed teeth scored ≥ 3 (TFI), ≥ 2 (TSIF) and 'mild' or worse (Dean's) will be considered to be of aesthetic concern. Analysis on dental fluorosis of aesthetic concern will be restricted to TFI, TSIF and Dean's indices as it is not easily determined from the modified DDE index.

In the report of [12], fluoride concentration in drinking water varied considerably within the country from very low (<0.10 mg/l) to more than 1.5 mg/l. Only little variation was found over the 10-year study period. Dental caries in both 5-year-olds and 15-year-olds decreased over the study period. An inverse relation between the risk of dental caries and fluoride concentration in drinking water was found in both primary and permanent teeth. The risk was reduced by approximately 20% already at the lowest level of fluoride exposure (0.125-0.25mg/l). At the highest level of fluoride exposure (>1 mg/l), a reduction of approximately 50% was found. Similar findings were found if analysis was limited to children residing in the same place during the entire study period.

[16] reported that at baseline, 666 children were examined; 543 of them (82%) were re-examined 2 years later. The adjusted dmfs increment was significantly lower in the intervention group compared to the control group by an average of 3.0

surfaces per child (95% CI = 1.2, 4.9), a prevented fraction of 31%. Adjustment for additional variables yielded caries reductions ranging from 2.3 to 3.5 surfaces per child and prevented fractions of 24-36%.

5.0 Discussion

The studies reviewed discovered that fluoridation of water can remarkably reduce the prevalence of dental caries in children as well as in adults' population, and decrease the mean DMFT. It was also observed that the decrease of the prevention of dental caries is more reported in children than in adults. There was also consistency from the proofs of the reviews that when more than 1ppm of fluoride is ingested, there would be evidence of fluorosis. Therefore, the developing countries should be encouraged to adopt the use of fluoride-based supplements.

6.0 Reviewer's Conclusion

There is a confirmation from the reviews that the prevalence of dental caries in children can be reduced by water fluoridation. Furthermore, a relationship exists between an ingestion of above 1ppm of fluoride and fluorosis.

6.1 Implication for Practice

In the practice of dentistry, specifically dental therapy, the fluoride usage should be encouraged in the prevention of dental caries, and the ingestion of fluoride should not exceed 1ppm.

6.2 Implication for Research

There is a dire need to conduct more studies on water fluoridation due to fluoride variation in countries. Moreover, there is also a need to ascertain the amount of fluoride to be ingested in developed and developing countries so as to avoid the occurrence of fluorosis. It was also observed that there is scarcity of relevant materials on the effects of fluoridation of community water in developing countries like Africa. Therefore, there is need for study in this area

.

References

[1] Adair, S. M., Bowen, W. H., Burt, B. A., Kumar, J.V., et al (2001). Recommendations for using fluoride to prevent and control dental caries in the United States.MMWR, 50(RR14), 1-42.

[2] Armfield, J. M. (2010). Community Effectiveness of Public Water Fluoridation in Reducing ildren's Dental Disease. Public Health Rep, 125(5), 655–664.

[3] Armfield, J. M., Spencer, A. J., Roberts-Thomson, K. F., & Plastow, K. (2013). Water uoridation and the Association of Sugar-Sweetened Beverage Consumption and Dental Caries in Australian Children. American Journal of Public Health, 103 (3), 494-500. doi: 10.2105/AJPH.2012.300889

[4] Beltrán-Aguilar, E. D. (2011). Use of Dietary Fluoride Supplements by Children Living in rlin, Germany, may have a Dose-response Preventive Effect Against Dental Caries, Regardless of their Use of Fluoridated Salt. Journal of Evidence-Based Dental Practice, 11 (2), 112-115.

[5] Buzalaf, M. A. R., & Levy, S. M. (2011). Fluoride Intake of Children: Considerations for Dental Caries and Dental Fluorosis. Fluoride and the Oral Environment, 22, 1–19, DOI:10.1159/000325101

[6] Chou, R., Cantor, A., Zakher, B., Mitchell, J. P., & Pappas, M. (2013). Preventing Dental

ries in Children <5 Years: Systematic Review Updating USPSTF Recommendation. Pediatrics, 132(2), 332 -350. doi: 10.1542/peds.2013-1469

[7] EBSCO Publishing. (2014). Fluoride. NYU Langone Medical Center. Retrieved February 19, 14, from http://www.med.nyu.edu/content?ChunkIID=229845

[8] García-Pérez, A., Irigoyen-Camacho, M. E., & Borges-Yáñez, A. (2013). Fluorosis and ntal Caries in Mexican Schoolchildren Residing in Areas with Different Water Fluoride Concentrations and Receiving Fluoridated Salt. Caries Res, 47, 299–308. DOI:10.1159/000346616

[9] Hausen, H.W. (2000). Fluoridation, fractures and teeth. British Medical Journal, 321(7265), 4-845.

[10] Hong, C. H. L., Bagramian, R. A., Nainar, S. M. H., Straffon, L. H., Shen, L., & Hsu, C. S. (2013). High caries prevalence and risk factors among young preschool children in an urban community with water fluoridation. International Journal of Paediatric Dentistry, 24 (1), 32-42. DOI: 10.1111/ipd.12023

[11] Iheozor-Ejiofor, Z., O'Malley, L. A., Glenny, A., Richard, M., Alam, R., Tugwell, P., Walsh, , Welch, V., & Worthington, H. V. (2013). Water fluoridation for the prevention of dental caries (Protocol). Cochrane Database of Systematic Reviews 2013, Issue 12. Art. No.: CD010856. DOI: 10.1002/14651858.CD010856.

[12] Kirkeskov, L., Kristiansen, E., Bøggild, H., von Platen-Hallermund, F., Sckerl, H., Carlsen, , Larsen, M. J., & Poulsen, S. (2010). The association between fluoride in drinking water and dental caries in Danish children. Linking data from health registers, environmental registers and administrative registers. Community Dent Oral Epidemiol, 38, 206–212. DOI: 10.1111/j.1600-0528.2009.00526.x

[13] Omale, J.J. (2006). Promoting dental health education as a panacea for the prevention of mmon oral diseases in Nigeria. Akoka Journal of Technology and Science Education, 3(1), 36-49.

[14] Petersen, P. E. (2003). The world oral health report 2003: Continuous improvement of oral alth in the 21st Century – the Approach of the WHO Global oral health program. Community Dental Oral Epidemiol, 31(Suppl.1), 3-24

[15] Petersen, P. E., & Lennon, M. A. (2004). Effective use of fluorides For the prevention of dental caries in the 21st century: the WHO approach. Community Dental Oral Epidemiol, 132: 319-321.

[16] Slade, G. D., Bailie, R. S., Roberts-Thomson, K., Leach, A. J., Raye, I., Endean, C., mmons, B., & Morris, P. (2011). Effect of health promotion and fluoride varnish on dental caries among Australian Aboriginal children: results from a community-randomized controlled trial. Community Dent Oral Epidemiol, 39, 29–43.

[17] Watt, R. G. (2005). Strategies and approaches in oral disease prevention and health motion. Public Health Reviews. Bulleting of the World Health Organization, 83, 711-718.

[18] Rozier, R. G. (1994). Epidemiologic indices for measuring the clinical manifestations of ntal fluorosis: overview and critique. Adv Dent Res., 8(1), 39-55.

Influence of Field Trip on The Development Of Students Interest Towards Studying Fine And Applied Arts

Onwuzo Ogonna .G.U. (Mrs.) and Odike Felicia .A. (Mrs.)

Federal College Of Education (Technical) Umunze
08033251788 Ogonnaonwuzo@Yahoo.Com
Federal College Of Education (Technical) Umunze, 07035183241

Abstract

The study investigated the influence of field trip on the development of students' interest towards studying fine and applied arts. Two research questions and one hypothesis were formulated to guide the study. All the J.S.2 students (totaling 310) from the three government owned secondary schools that offer fine and applied arts in Orumba South Local Government area in Anambra state were used. Mean and standard deviation were used to analyse the two research questions while Z-test was used to analyse the only hypothesis used for the study. Result of the study showed that; field trip increased students interest towards studying fine and applied art theory and practicals. Male interest towards studying fine and applied art after embarking on field trip is slightly higher than their female counterpart but the difference is not significant at 0.05 alpha level under 56degree of freedom. Recommendations were given.

Introduction

Art is a human conception made manifest through the skilful use of a medium. Art is like life; it is everywhere and is meant to give pleasure and joy to human beings. Fine and applied arts which is a branch of art is art forms that creates works that are primarily visual in nature, it is an activity that translates an idea into a blue print for something useful.

Uzor [10] asserted that scientists can invent technologies, manufactures can make products engineers can make them function and marketers can sell them but only fine and applied artists can combine insight into all these things and turn a concept into something desirable, viable and commercially successful and add value to people's lives.

In Nigerian secondary schools, fine and applied art education is studied under sculpture, ceramics, textiles, graphics, painting and craft. The role of fine and applied art can not be over emphasized. Wamgboje [9] posits that it deals with the emotions as well as the intellect of man. The expression of ideas feelings and mood in a relaxed atmosphere, the opportunity to solve problems in an individual way are attributes which fine and applied art brings to the curriculum. For short fine and applied art is a subject whose value when properly channelled to their most effective use, should play a major role in shaping man's general development so that he can live a full, contented and balanced life.

Regrettably fine and applied art has not been adequately appreciated in Nigeria. Egonwa [3] blames the problems of art in Nigeria on official injustices meted to the subject by those in authority. Among the injustices he listed was: Negative value orientation of parents, teachers, school head and administrators.

Mkpa [4] traced the social and moral decay in our society to neglect of importance of art in our school. This has

adversely affected the interest of secondary school students towards studying fine and applied art.

The method adopted by a teacher to communicate ideas to students can affect his interest and performance in the subject being taught [8]. Among the methods recommended for teaching fine and applied arts is field trip. Unfortunately, greater number of art teachers scarcely adopts it in teaching.

Field trip method of teaching is an educational visit, a journey made by a group of people, often students to study something in its natural environment (Abimbade 1997). It is an excursion taken to the actual location being taught for the purpose of making relevant observation and also for obtaining some specific information [1] about a particular population or phenomenon and experience (Obiajulu and Ezenduka 2013) which ordinarily are not available within the conventional classroom or studio.

During art excursion, students are encouraged to observe, learn techniques and styles of rendering, collect materials, take photograph of relevant works/scenes, ask and answer questions on the spot and appreciate works of art. Thus, increasing and improving their ability to perceive analyse and critique art works.

Efebo (1999) stated that the use of field trip enables students to become creative, learn to observe things better and enhance their listening skills. Similarly Nzeribe and Sawa (2002) asserted that field trip offers students opportunity of seeing the real situation of things they were taught in class thus making topics or concepts more vivid and retention better.

Futhermore Agbem [11] asserted that field trip promotes intrinsic rather than extrinsic motivation in students. This implies that students who participate in field trip receive satisfying intellectual thrill or self satisfying record.

Following these assertions, the question is, if field trip is applied in teaching fine and applied arts in secondary schools, will it positively or negatively influence students' interest toward studying art?

Purpose Of Study

The study sought to find out:

1. The influence of field trip on the development of students' interest towards studying fine and applied arts theory.
2. The influence of field trip on gender on the development of students interest towards studying fine and applied art practicals.

Research Questions/Hypothesis

1. What is the influence of field trip on the development of students interest towards studying fine and applied art theory?
2. What is the influence of field trip on gender on the development of students' interest towards studying fine and applied art practical?

Ho: There is no significant difference between the mean influence of field trip on the development of male students interest and female students interest towards studying fine and applied arts ($P<0.05$).

Design of the Study

The design employed in this study was a descriptive survey. The population consisted of all the junior secondary school two (J S S 2) students from the three (3) Government owned secondary schools that offer fine and applied art education in Orumba South local government area of Anambra state numbering 184 females and 126 males respectively. A total number of 310 students made up the population used for the study.

All the students used for the study took a field trip to all the departments in the school of fine and applied arts, federal college of education (T) Umunze. After that a researchers developed structured questionnaire on influence of field trip on development of students' interest towards

studying fine and applied arts. The instrument was validated by one expert in measurement and evaluation and one expert in art education. Direct approach was used in administering questionnaire to ensure 100% return. The two research questions designed in 5 point like scale were analysed with mean and standard).

deviation while hypothesis was tested with Z text at alpha level of 0.05.

For the two research question 3.5 was used as the cut of point. Thus any response with mean score 3.5 and above was regarded as accepted (agreed) while response below 3.5 was rejected (i.e disagreed.

Research Question 1

What is the influence of field trip in the development of secondary school students interest towards studying fine and applied arts theory?

Table 1: Mean Response of Influence of Field Trip on the Development of Students Interest Towards Studying Fine and Applied Arts theory?

S/N	ITEMS	$\bar{X}$	SD	Remarks
1	My engagement in field trip enabled me to develop interest in learning how to observe, understand and critique art	4.48	0.84	accepted
2	I like staying in art class to study concepts in fine and applied arts after participating in field trip	4.2	0.95	accepted
3	Work of paintings I saw during field trip has motivated me to develop interest in studying art movements and their styles of rendering.	3.85	1.07	Rejected
4	Since I came back from field trip I like spending my leisure time in solving problems in fine and applied arts.	3.3	1.17	Rejected
5	Since I came back from field trip, I derive pleasure in studying Nigeria artistic heritage – Nok, Benin, Ife and Igbo Ukwu art	3.63	1.06	Accepted
6	I have developed interest in art appreciation works of art after participating in field trip.	2.26	1.06	Rejected
7	Field trip to art institution increased my interest to study about great Nigerian contemporary artists	4.2	0.97	Accepted
		$G\bar{X}$=3.70	GSD=1.02	

The grand mean is 3.70 while grand standard deviation is 1.02. The table above revealed that items 1,2,3,5 and 7 scored mean above 3.5 which fell under accepted

region, while items 4 and 6 score a mean below 3.5 which is rejected. Overall result show that majority of the respondents are of the view that field trip has a positive influence in the development of students interest towards studying fine and applied art theory

Research Question 2:
What is the influence of field trip in the development of students' interest towards studying fine and applied art practicals?

Table 2: Mean Response Score of the Influence of Field Trip on the Development of Students Interest Towards Studying Fine and Applied Art Practicals?

S/N	ITEMS	$\bar{X}$	SD	Remarks
1	My participation in field trip has increased my interest in producing craft work with "found" objects.	4.16	1.01	Accepted
2	Field trip has aroused my interest in learning how to design posters and logos	4.30	0.98	Accepted
3	As a result of engaging in field trip my interest in carving has increased greatly	4.28	0.94	Accepted
4	Ceramic wares I saw during field trip has aroused my interest in learning pottery making.	3.93	1.05	Accepted
5	Since I came back from field trip I spend more time learning how to do tie dye and cloth weaving.	2.11	1.14	Rejected
6	My interest has increased greatly in print making as a result of what I learned during field trip.	3.18	1.26	Rejected
7	Participation in field trip has increased my interest in doing painting	3.01	1.19	Rejected
8	After taking field trip to art institution my interest in life and general drawing has remarkable increased.	3.66	1.14	Accepted

Grand X = 3.58; Grand SD = 1.09

Result from table 2 show that item 1,2,3,4 and 8 has mean scores above 3.5 respectively. On the other hand, items 5, 6, and 7 scored mean below 3.5 respectively and they fall within rejection region. Overall the grand mean is 3.58 while the grand standard deviation is 1.09

Hypothesis 1: There is no significant difference between mean influence of field trip on male and female students interest towards studying fine and applied art practicals.

Table 3:
Z –Test of difference on the influence of field trip on male and female students interest towards studying fine and applied art practicals.

Variable	NO	$\bar{X}$	SD	df	Standard error	Z-cal	Zcrit	Decision
Male Interest	126	3.62	1.05	56	0.124	0.403	1.96	N.S
Female interest	3.57	1.02						
N/B = NS – not significant at 0.05 alpha level								

Data in table 3 show the calculated Z score of 0.40 at 56degree of freedom. Although the mean score of male interest of 3.62 is higher that that of female (which

is 3.57), the difference in the mean score is not statistically significant P<0.5. This is because the calculated Z value of 0.40 is less than critical value of 1.96. Therefore the null hypothesis is accepted. This implies that the interest of male and female does not differ significantly remarkably after their participation in field trip.

Discussion

The findings in table 1 shows that, majority of the items have mean scores greater than 3.5 which is the cut off point used for the study. Most of the students where of the opinion that field trip increased their interest in studying; how to observe, understand and critique art works, about art movements and styles, Nigerian artistic heritage and history of great renowned artists. Similarly most students agreed that due to the increase in their interest in art after field trip they no longer absent themselves from taking fine and applied art lessons. These responses buttress the fact that field trip has made a remarkable influence in students' interest towards studying fine and applied art. This finding is in agreement with the observations made by Abimbade (1997, Efebo (1999), Nzeribe and Sawa (2002) and Agbem (2013 that field trip increases students interest to learn.

It is interesting to note that few students responded that field trip did not influence their interest towards studying art. This response can be attributed to factors like peer influence, perceptual differences among students and non adherence to pre-excursion activities by teacher. It is of paramount importance to brief the students as to the purpose of the field trip, what to look out for, and materials they should take along with them and behaviours expected of them during the trip. These go a long way to motivating them for the trip.

The result in table 2 showed that field trip has a positive influence on students' interest in studying fine and applied art practicals. A close look at the grand mean score of 3.58 reveals that the extent of interest is quite low. This may be attributed to the technique adopted by excursion guide during the field trip. The method of interaction between the guide and students has a lot to play in actualizing the objective of the exercise. Students should be actively involved during art excursion. They should be allowed to visualize, touch, manipulate materials and operate machines where necessary. This will help in making learning task meaningful and interesting to the learner.

The result of the study on table 3 revealed that there is no significant difference between the influence of field trip on male and female interest towards studying fine and applied art practicals, because Z cal of 0.40 is less than Z-critical of 1.96 at 0.05 alpha level of significance under 56 degree of freedom. It is worthy of note that both male and female scored mean above 3.5 which indicated a positive influence of field trip on their interest in fine and applied art practicals. This is in line with Uba (1995) assertion that students (both male and female) have strong desire to go on field trip because it increases their interest towards studying fine and applied arts.

The table also revealed that male interest is higher than that of female with mean score of 3.62 (for male) and 3.57 (for female). This finding is in disagreement with Okafor (1991) who posited that female students are more fascinated by pleasurable trip to places where they gain first hand information of what teacher would have taught them using other methods of teaching.

A close examination of the table also showed that the positive influence made by field trip on both the male and female student towards studying fine and applied art is not high nor significant. This can be traced to students learning style Sarasin (2001) revealed that students have different learning style. Thus those whose preferential mode of learning is tilted

towards abstract learning would perceive field trip as a waste of time and resources.

On the other hand, if majority of student who embarked on field trip were visual and tactile learners, their perception and interest on the subject will be similar and positive.

The implication of the study is that since many secondary school students shy away from studying fine and applied arts, it is necessary that students learning style be considered and accommodated in teaching – learning process.

Again, ii is of great importance that field trip be frequently used by fine and applied art teachers since it increases the interest of students towards studying the course. Teachers should source for relevant places of interest that are not too far from school environment and take student on excursion there. Failure to be the time will come when studying fine and applied art which helps to awaken child's creative potential will be completely erased from the tine table due to non enrolment of students in the subject.

Recommendation

The following recommendations were made:

The use of field trip in teaching fine and applied art should be emphasized in secondary school curriculum.

1. School administrations should encourage art teachers to adopt field trip in teaching fine and applied arts.

Parents should encourage their children whenever they are to embark on field trip by giving them financial and material support.

Excursion guides should make the exercise interesting and meaningful by encouraging active participation of the students.

Art teachers who organize excursion should ensure that the field trip fits solidly into current lesson plan, ie. The subject matter being studied at that time.

Conclusion

This study highlighted the concept of field trip and its importance to teaching and learning especially in fine and applied arts. It revealed that the use of field trip increases the interest of students towards studying fine and applied art. It recommended that field trip should be use more often in teaching of fine and applied arts.

References

[1] Abdullahi, A. (1982) *Science Teaching in Nigeria*. Ilorin: Atoto Press Ltd. Abimbade, A.(1987). *Principles and practice of Educational Technology.*

[2] Efebo, E.B. (1999). *Effective Teaching. Principle and Practice*.Paragraphics. Port Harcourt.

[3] Egonwa, O. (2001) *The development of Art and Culture sub-sector for Employment Generation In Delta State*. Retrieve from http.www.deltastate.gov.ng/bureaucrathtm on 20th February 2013.

[4] Mkpa, M. (2003) *Refocusing Nigerian Education System For Nascent Democracy*. A keynote Address presented at 5th National Biennial Conference of school of Education, Nwafor Orizu College of Education, Nsugbe.

[5] Nzeribe, A.C.B and Sawa, M.M (2009). *Principles and Method of Teaching*. Awka Marpat Educational Research and Publishers.

[6] , A.N. and Ezedike, M.M (2013). Field Trip: An Effective Approach For The

Teaching of Ecology in Secondary Schools. Journal of Education For Proffessional Growth. Vol. 8(1) July. Association of Educationists For Professional Growth in Nigeria.

[7] Sarasin, L.C. (1999) *Learning Style Perspectus. Impact In The Classroom*. Medison At Wood Publishing.

[8] Uchendu, O.G. (2005) *Effect of Co-operative/collaborative Interaction In Problem BasedLearning (PBL) Context On Students Achievement And Interest in Physics*. Unpublished P.h.D Dissertation. Submitted to The Department of Curriculum Studies/Educational Technology. University of Port Harcourt.

[9] Wamgboje, I. (1982). *A Textbook On Art For Junior Secondary Schools*. Evans Brother (Nig)ltd.

[10] Uzor, C. (2013) *Influence of visual Art On the Development Of Reading Culture Among Pupils Between Ages 10-12*. An Unpublished PDE Project submitted to the school of Education, Federal College of Education (Technical0 Umunze.

[11] Agbem, S.S. (2013) *Adopting Field Trip Strategy in Teaching Ecology Effectively* in Ango, M.L; Odayemi, Y.O; Oke M.G; Nwosu, A.A and Etokebe, I.J. (eds). Strategies for Effective Teaching and Learning of Biology Focus on Ecology. STAN Biology Series, 2003.

Instructions for Authors

WAJIAR provides a multidisciplinary forum for the publication of original research and technical papers, short communications, state-of-the-art developments in Information and communications technology, bio-medical informatics, computers, mathematics, control and information technology, physics, industrial electronics and engineering, Industrial chemistry, general technology, rocketry, space and astronomy, earth science, oceanography and the environment with special emphasis on the application of communications and information technology to these fields of importance in our modern civilization. The journal will review papers on advances, techniques, practice and application of information and communications technology in these areas.

- Economics, Statistics and Mathematic
- Information Technology & Applications
- Electronics and Computer Engineering
- Computer networks, Satellite & communications Engineering Research
- Industrial Computer applications Today
- Computer and Electro-Mechanical Maintenance
- GPRS and Remote Sensing
- Robotics ,Telemedicine & Remote Medical Monitoring
- Artificial Intelligence & Expert Systems Development & Applications
- Developments in Forensic Science Research
- Information Assurance & Network Security: The African Dilemma
- Space Information Systems & Rockery : which way for Africa
- Video and Teleconferencing Innovations for Deployment in Africa
- Telecommunications Technology & 4G Applications
- Biotechnology
- Agriculture , Food Technology & Processing Environmental Technology & Impact Analysis
- E-Waste Management & Environmental Protection
- Management Science & Operations Research
- Wireless Technology, GSM and 4G Applications
- Alternative ,Grid and Green Energy Solutions for Africa
- Converting Academic Research in Tertiary Institutions for Industrial Production
- Nano Technology

WAJIAR is an international Journal of Science and Technology and is published quarterly in February, May, August and December.

Key Objectives*:*

provide avenue for the advancement, dissemination of scientific and technology research in the fields of science and technology with special emphasis on the deployment of Information & Communications Technology as an enabler and solution tool.

Versions:

Two versions of the journal will be published quarterly (electronic version posted in the web and hardcopy version**.**

Submission

Typescript and soft copy in MS-word format should be submitted by email to: Info@wajiaredu.com. Typescripts should be written in English, double-spaced and

single-sided on either Quarto or A4-sizeed sheets, and should be numbered beginning with the title page. The first page of an article should contain:

i) The title of the paper, the name(s) and address(s) of the author(s)
ii) A short title not exceeding 45 letters with space

An abstract of 50-200 words should follow the title page on a separate sheet.

Text

Headings and subheadings for different sections of the paper (e.g. Introduction, Methods, Results, and Discussions) should be clearly indicated. Units of measurement, abbreviations and symbols should follow the international system of units (SI), Equations and formulae should be typewritten or word-processed. Equations should be numbered consecutively with Arabic numerals in parentheses on the right-hand side of the page. Special symbols should be identified in the margin.

Tables and Figures

Tables should be given short informative titles and should be numbered consecutively in Arabic numerals. Tables will be reproduced directly from the typed or word-processed softcopy. Figures in a form suitable for reproduction should be submitted separately from the text as original drawings in Indian ink, or as high contrast sharp photographs on glossy paper. Lettering on figures should be proportional to the size of the figure to ensure legibility after reduction. On the back of each figure, the orientation of the figure and the author and figure number should be cited consecutively in the text and a list of short descriptive captions should be provided at the end of the paper.

References

References should be cited in the text using a number in square brackets in order of appearance. The references are listed at the end of the paper in numerical order.

General Information

***Proofs*:** Proofs will be sent to the nominated author to check typesetting accuracy. No changes to the original manuscript are accepted at this stage. Proofs should be returned within seven days of receipt**.**

Reprints: reprints may be ordered (pre-paid) at prices shown on the reprint order form which will be sent to the author together with the proofs.

Page Charge: Please note that there will be a page charge of N20,000 or $100 (Twenty thousand naira or One Hundred American Dollars only) for each article accepted for publication in the journal.Annual Subscription is pegged at N20,000 or $125 per annum for four volumes. Electronic copies will be free access at our website. Subscription for the printed version will be completed via our Website www.wajiaredu.com. Subscriptions can also be sent via the journal's email address: www.wajiaredu.com/webmail / info@wajiaredu.com .ISSN: 2276-9129

West African Journal of Industrial & academic research

West African Journal of Industrial & Academic Research

Publications Office:
9-14 mbonu ojike Street
Ikenegbu, Owerri, Nigeria
Tel: 234 81219 41139, www.wajiaredu.com

International office:
255 North D Stree
San Bernardino, CA 92401
909.884.9000

Subscription Application Form

Name of Subscriber:_____
Institutional affiliation:_____
Mailing Address to send copies of journals _____
_____
Email Address:_____Tel:_____

Version of Journal requested: (a) hard copy N20,000 or $125 ☐
(b) electronic N10000 or $63* ☐

Method of payment:
Wire Transfer ☐
Visa Card
Master Card ☐
Direct payment into our Diamond Bank
Account No:. 0024189096 Douglas Rd branch, Owerri ☐
Bank Draft
Tick ✓

All subscription Application should be forwarded to: info@wajiaredu.com
Subscribers Signature: _____ Date: DD/MM/YYYY___/____/___
*WWW.WAJIAREdu.com is free access