Deploying Trusted Cloud Computing for Data Intensive Power System Applications

Mary-Jane Sule, Maozhen Li
Dept of Electronic & Computer Engineering
Brunel University London
UK
mary-jane.sule@brunel.ac.uk
maozhen.li@brunel.ac.uk

Gareth A Taylor
Brunel Institute of Power Systems
Brunel University London
UK
gareth.taylor@brunel.ac.uk

Simon Furber
Computing Services
Brunel University London
UK
simon.furber@brunel.ac.uk

***Abstract*- Cloud computing deployment is gaining popularity among sensitive mission-critical sectors like the energy sector. Cloud computing can provide cost effective scalable deployment of ICT services and infrastructure to the energy sector. However, the security, confidentiality and integrity of data are paramount and are of great concern to the energy sector. This paper presents the deployment of trusted Cloud computing for mission critical applications in the energy sector. The research presented in this paper simplifies the integration of trusted platform module based integrity measurement into commodity cloud infrastructure by eliminating the need for "custom" software and patches; it also enhances instance-level security by including a distributed file and directory integrity checker for added security. The deployment of trusted cloud computing using the Eucalyptus Cloud software on server-grade hardware is discussed, as well as the results of a comparative evaluation of the additional overhead in instance creation/start-up based on a simulation of low, medium and high security settings. The trusted cloud computing infrastructure is also currently available for deployment and testing by power system application developers and users.**

***Index Terms*--Cloud computing, energy sector, integrity, power system applications, security, trusted computing ,trusted platform module.**

I. INTRODUCTION

Cloud computing has made scalable computing resources more widely available and has also achieved economies of scale; however, as noted in [1- 4] a global challenge to its full deployment and adaptation are the security and integrity of various components such as the Cloud Infrastructure (CI) and the deployed instances/virtual machines.

NIST [5] defines Cloud Infrastructure (CI) as the combination of the hardware and software that enable cloud computing. Various authors, including [1], [2] and [5], further defined Cloud infrastructure as a Service (CIaaS) as one of the cloud computing deployment models that provide access to virtualised hardware services like servers, disk space and memory to clients for software deployment/development. The CIaaS service enables the deployment of the instances/virtual machines that are the "work-horses" in Cloud computing.

Mission critical services such as the electrical power grid require on-time availability and reliability of scalable computing resources, which is only possible through the deployment of Cloud computing. However, more needs to be done with regard to the security and integrity of the cloud infrastructure and the virtual machines (instances) running on the "cloud". There is also a need for the secured processing of data whether on the "cloud" or in the traditional computing environment. The security of the data and applications can never be over-emphasised as the energy sector relies heavily on efficient and secured data [1-4].

Cloud computing can facilitate and simplify the exchange of data between the Distribution Network Operators (DNOs) and the Transmission System Operators (TSOs) as required in the UK by National Grid (NG) [6]. In a cloud-based environment, the integrity of the entire UK power system would depend on the ability of DNOs/TSOs to update and maintain only sections of data related to their equipment/network. The exchange of data between DNOs and TSOs is greatly facilitated by the adoption and use of a common file exchange format. However, the data is of great value (potentially highly sensitive to national security) as they describe the state of portions of the national transmission and distribution networks.

The energy sector requires a trusted cloud computing infrastructure that can guarantee secure ownership and integrity of the uploaded data even when it is decrypted for processing. The research presented in this paper focuses on intrusion detection (integrity / trust) and security of the virtual infrastructure (architecture) as a possible approach to addressing security when deploying Cloud computing [7].

A group of DNO or TSOs (end-users) carry out the up-load, validation and storage of data in the secure storage locations (EBS storage volumes). Typically the end-users operate exclusively over the secure interface of applications such as an SSL-enabled web-interface. Direct attestation/verification of the Cloud Infrastructure's security and integrity by end-users (DNO/TSOs) is possible if enabled by both the CI provider and the application providers (NGs).

The NGs are responsible for creating the instances from the supplied images, installing and configuring additional or needed applications. As power-users, NGs have secure shell (SSH) access to the CI; this is useful for conducting security / integrity testing and verification.

Brunel University as the infrastructure provider is responsible for setting up the secured images and volumes from which the instances are created.

Fig.1. shows a prototype implementation of a trusted cloud computing deployment on the Brunel University computer network where both Trusted Computing (TC) integrity measurement/verification based on the Trusted Platform Module (TPM) [8] and intrusion detection using Advanced Intrusion Detection Environment (AIDE) [9] were

978-1-4673-9682-0/15/$31.00 ©2015 IEEE

Authorized licensed use limited to: Cranfield University. Downloaded on June 19,2025 at 13:44:06 UTC from IEEE Xplore. Restrictions apply.

integrated into a Eucalyptus based cloud platform. The prototype demonstrates the levels of containment used to provide infrastructure security, while also providing a form of integrity and trust for the clients using the platform.

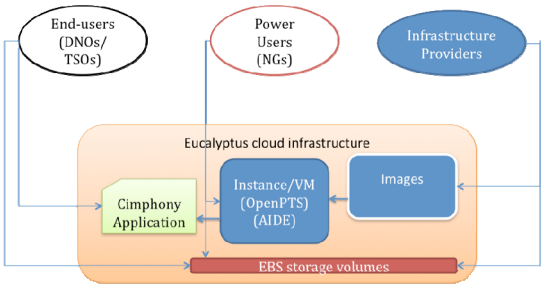

Fig.1. Deployed system on Brunel University Network

This research is in collaboration with industry partners Open Grid Systems [10] and NG [6]. The prototype has been made available to the industry partners for application deployment and testing. The result suggests little or no overhead from the added security mechanisms.

II. Secure and Trusted Cloud Computing

Considerable researches have been carried out in the area of Cloud computing security and integrity but still more needs to be done as regards the security and integrity of the cloud infrastructure and the virtual machines running on the "cloud".

Researchers [11] investigated intrusion detection in Cloud computing middleware only without adequate consideration for Cloud Infrastructure and virtual machines. Researcher [6] discusses a technique of grouping nodes, Cloud implementations such as Eucalyptus implements a similar functionality called security-groups.

Berger et al [12] researched extensively on how to prevent data leakage, virus spread between instances / nodes and misconfiguration of tasks; they discussed some security solutions in cloud infrastructure based on hierarchical administration, controlled access to network based on security labelling and grouping among other solutions, [7] focused only on virtual data centres and do not extend integrity checks to applications or services.

Reference [13] rightly put it, Cloud computing is an amalgamation of different computing technologies, therefore its security and trust challenges are in no way "new" or unique. These challenges, which border on trust, cloud architecture, identity management, software attack, data protection and availability are more pronounced as transactions are sometimes initiated even with faceless strangers [13 – 16].

In Trusted Computing, the chain of trust from the TPM hardware device through the firmware (BIOS), boot loader (kernel) and operating system of the cloud middle-ware may be extended to cover virtual storage devices. In the trusted cloud, the attestation of the cloud-infrastructure (based on the TPM hardware chain-of-trust) from a running VM is carried out as a single TC operation targeted at the local controller over a secure-shell connection. The use of a local secure-shell connection reduces the possibilities for network based man-in-the-middle attacks. Similarly, the inclusion of a software based virtual TPM (vTPM) device within the instances allows a new and unique chain of trust to be built for the kernel, operating system and software components of the instance.

Fig. 2 shows the implemented architecture of the secure and trusted cloud where a chain-of-trust from the hardware/BIOS guaranteeing that all the software components of the cloud-infrastructure are measured before being loaded.The Trusted Core Service Daemon (TCSD) is used to export trusted services from the physical TPM device into the operating system of the cloud-infrastructure.

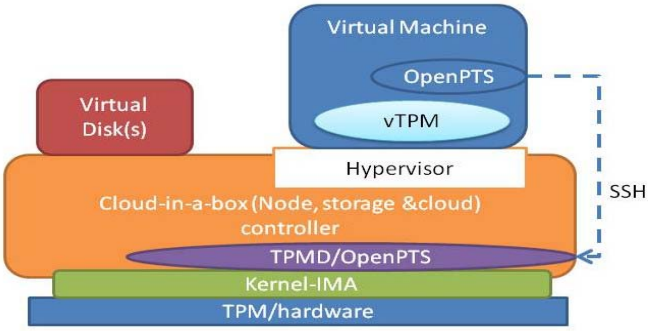

Fig.2. Architecture of the secure trusted cloud

The Open Platform Trust Services (OpenPTS) [17] application is used to implement the attestation procedure. OpenPTS runs in either collector or verification modes and can carry out remote attestations using the standard secure-shell application for transportation and protection against man-in-the-middle attacks. In the collector mode, openPTS collects and maintains a trusted manifest/database of measurements to be examined during the verification process.

The trusted manifest/database of measurements is made available within the VM/instance and used during the remote attestation of the cloud-infrastructure by openPTS when running as a verifier. In the reported work, an instance/VM is always a TC verifier and the virtual TPM (vTPM) installed within the VM is only required to satisfy a dependency requirement of the openPTS application, also installed in the VM.

A. Securing Cloud Platforms with TC and intrusion Detection

Currently, security in most Cloud computing platforms is limited to the ability to partition/group instances by owners, or hierarchical levels of administration. They do not include or enable support for Trusted Computing integrity measurements/verifications based on Trusted Platform Module (TPM), an industry standard for computing hardware integrity measurement and testing, that depends on special hardware storage of cryptographic keys. Cloud platforms also do not include adequate intrusion detection mechanisms for certifying that the instances/virtual machines have not been tampered with.

Authorized licensed use limited to: Cranfield University. Downloaded on June 19,2025 at 13:44:06 UTC from IEEE Xplore. Restrictions apply.

TC provides an added level of trust related to the cloud-infrastructure as it allows measuring the collective integrity of the hardware platform, firmware and operating systems components responsible for booting.

Integrating TC into cloud implementations would allow cloud administrators to measure and verify infrastructure integrity; however, the end-user integrity measurement/testing of the underlying infrastructure require some additional mechanism such as a secure channel for end-users to access the cloud platform.

TC based on TPM is useful for measuring system integrity; it typically cannot detect exactly what was changed or locate the changes to exact file, the addition of a file and directory intrusion detection system allows fine-grain examination/characterisation of the changes that occurred.

Intrusion detection software such as Advanced Intrusion Detection Environment (AIDE) provides file level integrity verifications (including permissions and attributes) based on stored hashes. A relatively small Linux system could easily have hundreds of thousands of files. A full scan and verification tend to be both processing-intensive and time-consuming as the hash must be recalculated for each file and compared to the stored value. The ability to limit the scan to certain selected files is quite useful and can significantly reduce the amount of time needed during verification.

The methodology used in securing the underlying cloud-infrastructure and instances for end-user verification involves the following steps:

- Enabling TPM hardware from BIOS/firmware: The cloud hardware is expected to include suitable TPM hardware.
- Enabling TC measurement related options on the Kernel layer. For Linux, this is by modifying the boot-loader options (adding IMA) and configuring a virtual file system (securityfs).
- Installing and configuring the operating system TPM related applications (trousers and openpts).
- Creating an SSH-only account for remote attestation by instances.
- Integrating TPM tools into the virtualised image
- Pre-seeding the OpenPTS verification database in the image with the keys from the Cloud-infrastructure.

B. Prototype Deployment

The Eucalyptus Cloud Software was chosen for this research based on the following features: it is open source which allows for further customisation and configurations, provides a user/management web interface with custom credentials, allows for re-write of the scheduling controller and provides strong internal security settings [2, 9, 17].

The Eucalyptus Cloud Software also allows the entire cloud infrastructure to be configured and deployed on a single computer (box). This "Cloud-in-a-box" technology is basically a CIaaS that provides basic functions like provision storage, network and security resources. Furthermore, it also includes auto scaling, cloud-watch and elastic load balancing, which are typically found in a fully functional "cloud".

The cloud software was deployed on an Intel donated hardware system with the following specifications: - 1 T HDD, 64GB memory, 40 processing-cores

The images running on the deployed system are based on 64-bit Ubuntu Linux operating system version 14.01/trusty, which have been further customised in the current research.

Eucalyptus provides some basic Cloud computing security on its platform such as secure socket layer (ssl) connections, user password among others that were activated on the platform.

TC measurements/verification based on the OpenPTS (Open Platform Trust Services) implementation and Intrusion detection based on AIDE (Advanced Intrusion Detection Environment) software were installed / configured on the images to further enhance security and trust of the images that would subsequently be used to deploy the instances.

C. TC Verification Process

The OpenPTS technology operates with one of the systems, that is, the cloud-in-a-box host system taking the role of the collector and the other system(s) (the instances) taking the role of the verifier.

The integrity measurements/verification provided by OpenPTS allows an end-user to verify that the cloud-in-a-box server, where the image is hosted (called the collector) is actually the right and secured one. The verification process is performed over a secure shell (SSH) connection based on pre-seeded keys at the verifier side.

The cloud-in-a-box server performs a trusted boot based on data contained within its Trusted Platform Module (TPM) hardware. TPM is a microprocessor chip built into a machine to enhance its security by integrating cryptographic keys into the machine; these keys provide authentication (proves the platform is what it claims to be) and attestation (platform is trustworthy and has not been breached). These keys are checked for consistency by the verifier.

With a suitable OpenPTS command syntax (–v option), the verifier can check up and compare the current values against a pre-seeded set. The result, which means the keys tally (success) or does not (failure) is reported to the verifier and on failure, it is also possible to configure more drastic action such as the immediate shut down of the instance/virtual machine.

A verification failure (reported by OpenPTS) is an indication of a variety of issues, including the possibility that the verifier is communicating with a different or rogue machine, booting from the wrong machine or even that the image has been tampered with or modified. This helps with checks to improve security and trust on a cloud-computing infrastructure while deploying an instance.

File level Intrusion detection is provided by AIDE, an integrity checker for files and directories, based on a variety of digest algorithms (md5, sha1, rmd160, tiger, whirlpool, sha512, etc). AIDE has the ability to check for inconsistencies in the file/directory attributes. Based on the required

Authorized licensed use limited to: Cranfield University. Downloaded on June 19,2025 at 13:44:06 UTC from IEEE Xplore. Restrictions apply.

speed/performance, the scan/verification may be limited to specific files and directories.

D. Hierarchical Security Model

Apart from the built-in security groups features in Eucalyptus, a hierarchical security model was also used to provide secure Cloud computing services to a group of researchers both within and outside the University. These researchers are categorized according to the following access levels:

a. Power Systems Cloud Infrastructure administrators – This category of users is responsible for providing secured images to be used by other users for their application /software. They have control of the underlying cloud infrastructure and can access the system on both ports 8443 and 8888 using the address https://powersystemscloud.brunel.ac.uk:8888/ or https://powersystemscloud.brunel.ac.uk:8443/

b. Power Systems Cloud Application Developer: The second category of users on this platform is responsible for creating instances (VMs) from the provided images and subsequently installs desired applications; these applications are in turn used by the end-users. They have no access to or control over the underlying cloud infrastructure and can only access the system using the address https://powersystemscloud.brunel.ac.uk:8888/

c. Power Systems Cloud Application Users: The third category of users on this platform is the end-users. Users in this category have only HTTP/HTTPS access to instances / applications running on the platform.

III. Evaluation

The integration of either Trusted Computing (TC) or intrusion detection with Cloud computing introduces performance overhead especially during boot up or in the process of setting up attestation or verification [10].The goal of the research experiment was to determine the overhead that could result from the introduction of either TC integrity measurement/verification or AIDE based intrusion detection/verification into an instance. The improved security appears to have limited and negligible overhead for single instances and it can therefore be concluded that it is not going to be noticeable until thousands of instances are started.

Table 1 shows the average boot-time recorded for each security level and Fig. 3 shows a graphical representation of the 21 instances deployed during the research experiment. These instances were classified into three broad security levels: low, medium and high. Where the low security group do not include TPM or AIDE and serve as an experimental control or baseline group. The medium group include only TPM based integrity measurements/verification.

The instances at start-up typically started the TPM-emulator device and setup the user-environment for remote verification of the CI platform. While the high security group include both integrity verification and AIDE intrusion detection, the instances start up the TPM emulator device and setup the user-environment for remote verification of the CI platform. The AIDE database is already pre-seeded, but the end-user verification process needs to be set-up as well.

From Table I, The control group had an average boot-time of 54.16 seconds, while the medium security group had an average boot-time of 55.38 seconds; the high security group had an average booth time of 56.81 seconds. The results shows that the overhead incurred including TPM based integrity measurements/verification into a cloud platform for this research is 1.22 seconds while the overhead incurred including TPM and AIDE based intrusion detection into a cloud platform is 2.65 seconds. This is further represented in Fig. 3, which shows the results obtained from the deployment of 21 instances at each security level. The maximum overhead between low and high security levels is between 3 and 4 seconds. The results suggest that the improved security overhead on the cloud platform is limited and capable of scaling to large numbers (thousands) of instances.

TABLE I
INSTANCES BOOT-TIME

	Low Security	Med Security	High Security
	Min:Sec.CenSec	Min:Sec.CenSec	Min:Sec.CenSec
1	00:53.32	00:55.58	00:56.81
2	00:54.11	00:55.32	00:57.01
3	00:53.78	00:55.35	00:56.66
4	00:54.21	00:55.14	00:57.18
5	00:53.81	00:55.28	00:56.59
6	00:53.63	00:55.54	00:57.09
7	00:53.54	00:55.13	00:56.54
8	00:53.78	00:55.20	00:57.01
9	00:53.92	00:55.22	00:56.61
10	00:53.63	00:55.01	00:56.67
11	00:54.88	00:54.91	00:56.90
12	00:54.84	00:55.51	00:57.21
13	00:54.39	00:55.49	00:56.69
14	00:54.51	00:55.44	00:56.90
15	00:54.10	00:55.78	00:56.72
16	00:54.14	00:55.00	00:56.66
17	00:54.50	00:55.26	00:56.87
18	00:54.41	00:55.70	00:56.83
19	00:54.77	00:56.22	00:57.02
20	00:54.80	00:55.78	00:56.61
21	00:54.23	00:55.03	00:56.51
Av Sp.	00:54.16	00:55.38	00:56.81

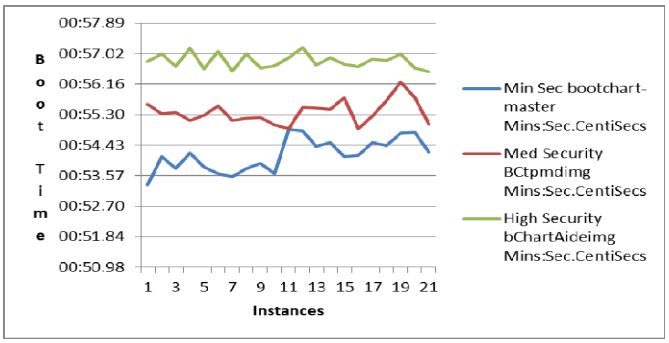

Fig.3. Boot time representation

Authorized licensed use limited to: Cranfield University. Downloaded on June 19,2025 at 13:44:06 UTC from IEEE Xplore. Restrictions apply.

IV. Conclusion

This paper presents and discusses a trusted cloud deployment especially suited for mission critical applications in the energy sector. The approach involves the integration of end-user accessible TPM integrity measurement/verification into the cloud platform/infrastructure without the need for "custom" software or patches.

Furthermore, security is enhanced by the inclusion of an instance-level file and directory integrity checker for selected files and directories. Using a trusted cloud computing infrastructure can guarantee trusted ownership and integrity of the uploaded data as it would ensure that each operator is provided with a diversified access model based on data sharing needs.

In a cloud deployment approach, individual organisations/users share a common cloud platform and sometimes not necessarily retaining control over their sensitive data or applications deployed on external infrastructure. The research work reported here provides additional levels of trust for cloud infrastructure which allows individual organisations/users to retain control of their sensitive data/processes. A working prototype of the secure trusted cloud deployed on the Brunel University London network has been made available to industry partners OGS and NG to deploy and test power system applications like Cimphony [10].

Further research and development of the proposed platform would demonstrate novel security measures for direct end-user's verification of cloud based services where end-users can dynamically and independently check that adequate data protection has been put in place on the shared resources.

Acknowledgement

This research is supported by the UK EPSRC under grant EP/K006487/1 and National Grid.

References

[1] M.Nelson (2009). "Briefing paper for the ICCP technology foresight forum cloud computing and public policy", [Online]. Available: www.oecd.org/dataoecd/39/47/43933771.pdf [Accessed: 16th March 2014].

[2] M. Armbrust, et al., "Clearing the Clouds away from the true Potential and Obstacles posed by this Computing Capability," Communication of ACM, vol 53, No. 4, pp 50-58, April 2010.

[3] R. Chalse et al., "A New Technique of Data Integrity for Analysis of the Cloud Computing Security," in Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, Mathura, 2013, pp 469-473

[4] S. Reiner et al. "Design and Implementation of a TCG-based Integrity Measurement Architecture." in USENIX Security Symposium, 2004, vol. 13, pp. 223-238.

[5] P. Mell and T. Grance (2011, Sept). "The NIST Definition of Cloud Computing". NIST [Online]. Available:http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.[Accessed: 28th October 2014]

[6] National Grid (2014) The Grid Code http://www2.nationalgrid.com/WorkArea/DownloadAsset.aspx?id=37040].

[7] K. Vieira et al.,(2010, July/August). "Intrusion Detection for Grid and Cloud Computing ", IT Professional, vol 12, no. 4, pp. 38-43, July/ August 2010 doi:10.1109/MITP.2009.89

[8] TPM http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

[9] AIDE http://aide.sourceforge.net/

[10] Open Grid Systems https://www.opengrid.com/content/

[11] K. Vieira et al., (2010, July/August). "Intrusion Detection for Grid and Cloud Computing ", IT Professional, vol. 12, no. 4, pp. 38-43, July/ August 2010 doi:10.1109/MITP.2009.89

[12] S. Berger et al., (2009, July). "Security for the cloud infrastructure: trusted virtual data center implementation". *IBM J. Res. Dev.* 53, 4 (July 2009), 560-571

[13] W.A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *System Sciences (HICSS), 2011 44th Hawaii International Conference on* , vol., no., pp.1,10, 4-7 Jan. 2011 doi: 10.1109/HICSS.2011.103URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5719001&isnumber=5718420

[14] NIST. 2011. Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security." National Institute of Standards & Technology. Accessed April, 2014 at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[15] M.R. Nelson, 2009. The cloud, the crowd, and public policy. Issues in Science and Technology Available: http://issues.org/25-4/nelson-2/ Accessed 1st December 2014.

[16] S. Kaur and P.S. Mann (2014, May) " A Review on Cloud Computing Issues and Challenges" Intl Journal of Research in Computer Applications and Robotics., Vol. 2 Issue 5 pp 63-68

[17] OpenPTS http://sourceforge.jp/projects/openpts

[18] D. Wallom, M. Turilli, A. Martin, A. Raun, G. Taylor, N. Hargreaves, A. McMoran, "myTrustedCloud: Trusted Cloud Infrastructure for Security-critical Computation and Data Managment," cloudcom, pp.247-254, 2011 IEEE Third International Conference on Cloud Computing Technology and Science, 2011

Authorized licensed use limited to: Cranfield University. Downloaded on June 19,2025 at 13:44:06 UTC from IEEE Xplore. Restrictions apply.