Towards an Efficient and Secure Educational Platform on Cloud Infrastructure

Sarfraz Nawaz Brohi, Mervat Adib Bamiah, Suriayati Chuprat
Universiti Teknologi Malaysia, Malaysia
nbsarfraz2@live.utm.my
abmervat3@live.utm.my,suria@ic.utm.my_

Jamalul-lail Ab Manan
Mimos Berhad, Malaysia
jamalul.lail@mimos.my

***Abstract*—Existing educational platforms are highly cost-consuming and inefficient in-terms of scalability, flexibility of infrastructures, availability, recovery, accessibility and security. Cloud computing is considered as a flexible business and technological model for providing an Efficient Educational Platform (EEP) due to its significant features. However, an EEP is not a complete solution required by Educational Organizations (EOs), they require Efficient as well as Secure Educational Platform (ESEP). Since cloud computing is an open access global technology, there are several security threats that might take place from malicious users. EOs are reluctant to trust and adopt this paradigm because of threats that can compromise the security of their confidential data. In this research paper, we describe the ICT related challenges faced by educational platforms and we emphasize the significance of cloud computing in enabling an EEP, finally we propose a conceptual model for developing an ESEP. Our contribution consists of several security tools and techniques such as Trusted Virtual Domains (TVDs), Security as a Service (SECaaS), Intrusion Detection Tools, Trusted Platform Module (TPM), virtual TPM (vTPM).**

***Keywords*- Efficient and Secure Educational Platform, Cloud Computing, Security and Trust Issues, TPM, vTPM, TVD, SECaaS**

I. INTRODUCTION

Education is a fundamental component in every country's development and building strong economy for-long term successful future. An EEP can empower the associated entities such as administrative staff, management, lecturers, and students to develop a workforce with high value and global skills. At present, majority of EOs across the world are deploying their educational platform on self-managed on-premises infrastructure which consists on number of servers that are managed by technical IT staff members within the organization. According to UNESCO [1], the institutionally hosted educational platforms are cost-consuming and facing several challenges regarding inefficiency of platform scalability, availability and recovery, software licensing, accessibility and system security. These challenges are further analyzed by our research and described in detail as follows:

A. Platform Scalability

Scalability is one of the on-growing challenges for EOs. If an EO suddenly requires to scale-up the their educational platform i.e. deployment of additional applications and data during the peak seasons such as starting of a new year admission or examination, their current infrastructure will be over-utilized and requires extra resources to be purchased including storage devices, processors, networking components etc, to deploy new servers. On the other hand, when peak season finishes and the EO returns back to normal season i.e. processing load is lower and additional severs are not required, consequently the infrastructure will be under-utilized. This clearly demonstrates that the current platforms are not flexible enough to accommodate new requirements such as scaling-up or down in cost-effective manner.

B. Availability and Recovery

An EO requires a solution that guarantees optimum availability, however a network failure or a natural disaster can turn into service disruption for a long duration. Consequently it may lead to Denial of Service (DoS) for several entities that are associated with that particular educational platform. Sometimes it requires outsourcing the work to a third-party troubleshooter to overcome the issues that may result into an increase of un-expected cost. EOs can never guarantee high availability of their system because even if platform don't face any threats, they need to conduct sessions for scheduled maintenance which will also lead to abortion of required services for some interval each time this activity is conducted. In some cases such as natural disasters (earthquake, tsunami, etc) the organizations platform can be destroyed and it may result in permanent loss of entire data and applications. To mitigate these issues and achieve business continuity, an EO needs to maintain a back-up recovery plan and implementation which is again an expensive solution.

C. Software Licensing and Upgrading

Third challenge is that an EO has to pay for high licensing cost of buying and upgrading their software. If there are demands for new software or upgrades for new courses within the faculty, university or college, an EO has to entertain the demands. An EO must be aware about latest software updates and need to keep its software up-to-date. Purchasing and licensing renewal cost of new software will dramatically increase the cost.

978-1-4673-4416-6/12/$31.00 ©2012 IEEE

D. Accessibility

At the on-premises educational platform, the required services through devices would have limited access capability in-terms of time, location and accessing device. This becomes an issue because the software development team normally assumes the PC/laptop as the standard accessibility medium. Hence, accessing via smart devices such as smart phones would encounter incompatibility and interoperability issues. Furthermore, the use of micro and digitalized technology is rapidly increasing and students are more comfortable to use smart phones, notebooks, tablets instead of PCs or laptop. Future systems must consider accessibility via smart devices from any location at anytime without any incompatibility, access time or location issues. Other issue that may happen is if an employee or students completing a part of work in the organization, they need to store the data in USB or any backup devices. Under, some unfavorable circumstance if the storage device is lost, all the work done will go waste.

E. System Security

System security is the most critical challenge faced by many EOs and they are required to implement appropriate security standards to avoid misuse and illegal access of their applications and information. The security threats can take place on an EO's system by outside or inside malicious attackers. In order to eliminate this issue, software development team must implement the system with appropriate strong security techniques. The successful implementation and monitoring of system security in the organization also requires expensive management and labor cost.

II. Significance of Cloud Computing in Developing an Efficient Educational Platform

Considering the limitations of current educational infrastructure, we require an EEP that must be flexible to exhibit the services of scalability, availability, recovery, accessibility and security in cost-effective manner. In other word, an EEP must be able to accommodate new organizational business requirements. Resources must be available on-demand at any time without any downtime, and they can be accessed from any location via any smart device. The resources must be secured i.e. applications and data of users' should be protected from illegal access. Considering the requirements for developing a EEP and looking at the feature of cloud computing such as scalability and flexibility, availability and disaster recovery, software on-demand and accessibility [1] [2], we can say that cloud computing will play an integral role in the development of a EEP.

A. Scalability and Flexibility

The primary objective for many EOs is cost saving and increase return of investment (ROI). According to proposed business model for cloud computing, users only pay for the computing resources they use. No need to buy new hardware, software or pay for maintenance and upgrading. In some existing solution, EOs need to purchase the infrastructure utilities at a fixed cost that normally became an issue of an under or over-utilized infrastructure. Being a client of cloud services, an EO can just acquire the basic resource such as applications, software or data storage size and they can scale up or down whenever is required on-demand. Scalability also allows for rapid escalations in demand at peak times such as at the start of academic year or exam periods. Therefore, there is no need to plan usage levels in advance [1]. In short, an EO can simply obtain the flexibility of expanding or shrinking their infrastructure without paying unwanted cost for new resources or management effort.

B. Availability and Disaster Recovery

Students are increasingly dependent on online services for learning and assessment. They should be given the best possible system availability. An EO's computing service department may aim to achieve 99.5% availability for its educational services such as the Learnfinity Management System (LMS). Such a requirement can be easily met by a service provider such as Google cloud services which offers 99.9% availability for its educational application suite and appears to enhance this target [1]. Moreover, Cloud Service Providers (CSPs) offer the required disaster recovery infrastructure and plan. They provide recovery system and replication of data at several geographical locations such as cities, countries or states that are permitted by legal law. CSPs also maintain procedures for accurate and reliable retrieval of data. Due to disaster recovery, backup plan and efficient troubleshooting tools used by CSP, EOs can assume that they are highly saved from facing downtime issues and loss of data due to.

C. Software on Demand

For the end users, apart from better availability and disaster recovery, there are other clear benefits of cloud-based services, particularly evident with the range of new applications being provided. These contain the latest tools and features from innovative companies such as Microsoft and Google [2]. Students and other entities from EOs can use office applications without having to purchase, install and keep these applications up-to-date on their computers [1]. It is the responsibility of a CSP to provide always the latest and updated applications to the users and whenever necessary update the software versions without requiring any interaction from the users. Beside the applications from third party industries, EOs can also deploy their applications such as Human Resource Management System (HRMS), LMS, and admission systems on CCI that can be accessed at anytime remotely without installing or configuring them. EOs don't need to worry about backing up or losing the data as it should be safely stored in cloud with large storage capacity provided. Technologies such as HTML5 will increasingly allow users to work offline when Internet access is intermittent [1].

D. Pervasive and Ubiquitous Accessibility

The systems deployed on a CCI, have ubiquitous and pervasive accessibility [2]. If employees or students from an educational organizations are always using the cloud based system and storing their data on cloud, they are not required to carry backup or storage device, their workload will be saved on

the cloud storage and will never get lost due to use of backup and recovery services and it can be accessed within the organization, home or across the border.

III. Barriers in Adopting the Cloud Paradigm

Although there are significant flexible and efficient features that cloud computing can provide to EOs. However, like an EO's existing internal infrastructure, security on a CCI is not trustworthy and it is rapidly growing concern that needs to be addressed [3]. When data of a client is on the datacenter of CSP, there are obvious chances of security, hack, theft and various malicious activities that can be performed by illegal users such as hackers. Cloud computing datacenter environment is overloaded with trust issues [6]. Before moving to the cloud, an EO need assurance that their sensitive information is protected from compromised security procedures, and their applications are available whenever accessed [4] [5]. Due to security and trust issues in cloud computing, EOs are not yet ready to adopt the paradigm of cloud computing which creates a major obstacle to leverage the significant advantages of cloud services for EOs.

A survey conducted by ECAR shows that two-thirds of those who outsource, cited their institutional culture as a real barrier to adopting alternative sourcing approaches and those who outsource, nearly three-quarters (72.1%) cited concerns about IT security in adoption of emerging cloud computing services [7]. No suspect that cloud computing can be key enabler for a developing an EEP however survey results clearly represent that EOs consider security as their main concern for not moving towards cloud based IT services and solutions. Since security is a vital factor for organizations policies, the education organization need to be guaranteed on provided security standards and procedures prior to the adoption of cloud services. In order to overcome the security issues. In this paper we have provided a conceptual model to develop an ESEP on CCI.

IV. Related Work

(Z. Yang, 2011) [8], suggested an open structure framework that can interoperate with external content and social service, it can also interoperate with enterprise applications such as CRM, ERP, Groupware, SharePoint, etc and client's applications such as twitter, g-mail, YouTube, etc at the data level by mapping mechanism. This open structure framework has four layers i.e. user experience, collaboration service, core service, and delivery platforms. It can make internal cloud and external cloud interoperate with each other if standards are followed. The core of the framework is the standard cloud structure, namely e-Education cloud. The overall structure of e-Education cloud can be subdivided into management subsystem and service subsystem. (R. Elumalai, V. Ramachandran, 2011) [9] proposed cloud based e-Content sharing service deployed in Google App Engine in order to serve the academic community by providing a common educational e-Content repository wherein the contribution is also from the academic community. This model is designed to distribute e-Contents in the form of text, audio and video files to the intended audience, which are contributed by various subject experts from academic community. These files are uploaded to cloud storage as a service layer by the administrator after the peer reviewing process. In order to access the e-Contents, the user is requested to register with the service. At the time of registration the user needs to provide a basic personal information such as their email Id, geographical position, mobile number along with a request to identify them as users or content providers. Once they have entered the requested details, a unique One Time Password (OTP) is dynamically generated and is sent to their mobile numbers and to their email Id's which can be used for confirming their registration. The OTP is formulated by the random number generation algorithm which generates the random number within the range of 100 to 99999. The generated number is sent as text message to the client's registered mobile phone through third party Web service for sending Short Messaging Service-(SMS). Once the number is validated, the content provider can upload the e-Resources in the cloud e-Content Sharing as a Service layer.

V. Attack Surface of a Cloud Computing Infrastructure

We have identified two major types of attacks on a CCI i.e. un-trusted malicious VM attack by malicious outsider, and insider's attack by a malicious cloud administrator as shown in Fig.1, indicated by red color lines.

A. Malicious VM / Outsider's Attack

Normally malicious VMs may be belonging to the competitor of the EO on cloud, or CSP. The objective of this VM is to infect the services of EO in order to issue a DoS attack for their systems. This attack may be carried out to threaten the reputation of CSP. A malicious VM can mainly attack in two methods i.e. attack directly on other VMs and affect the client applications with viruses, malwares, Trojan horses or worms, or attacking on the host OS, if host OS is compromised, attacker can exploit the hypervisor and physical layer to misuse the client VMs and data. These kind of attacks can destroy the overall computing infrastructure because host OS is managing the hypervisor that is responsible for providing significant tasks for the VMs such as start, shutdown, pause and restart the VMs, monitor and modify the resources available for the VMs, monitor the applications running inside the VMs, view, copy, and modify the data stored in the virtual disks assigned to the VMs. This enables the host to monitor all the network traffic for all its VMs [10]. In-case if a host is compromised then the security of the VMs is under question. On the other hand, malicious VM can also change the configuration of underlying hardware and may try to steal the confidential data of EO. Hence measurement should be taken when configuring the VM environment so that enough security standards should be implemented which avoids the host being a gateway for attacking the VM [10], and physical layer must be protect by illegal access as it should be resistant to any malicious software activity.

B. Malicious Administrator / Insider's Attack

One of the primary security concerns in cloud computing is that the customer loses direct control over potentially business sensitive and confidential data. This needs more attention because the CSP is outside the trusted domain of customer [12]. The risk of a malicious insider is one of the most dangerous security threats. The cloud security alliance report lists malicious insiders as the number three top threat in cloud computing [11]. Clients are not aware and fully trusting the security technique used by the CSP when their data is on open access cloud computing platform. They believe even if their data is protected from outsider's attack but how about insider's attack. It is possible that malicious cloud administrator may, retrieve, view and misuse the confidential data of an EO. In order to gain the trust of EOs, CSP must provide them trustable security standards that ensure the protection of their data-at-rest.

VI. Our Contribution: Efficient and Secure Educational Platform (ESEP) on the Cloud Infrastructure

To address the issues on CCI, we have designed a conceptual model of an ESEP on the public CCI that is shared by multiple tenants including trusted and un-trusted users. Trusted users are the EOs who has signed a well-defined SLA with the CSP to use the cloud service delivery models such as SaaS (MicrosoftLive@edu, LMS, HRMS, OpenOffice), PaaS (GoogleAppsEngine, Microsoft Azure), and IaaS (Storage-as-a-Service) on pay-per-use billing pattern accessing via using smart devices such as Notebooks, Smart phones, Tablets etc. Un-trusted users refer to general public who are registered online with the CSP for using some shared service such as web-mail, media players, games etc as shown in Fig.1 the services of a an EO are running on VMs, we have illustrated the use of two VMs for the EO, both VMs consists on guest OSs and applications that are configured on Apache Tomcat server along with a DBMS such as MySQL. The un-trusted users are also assigned with VMs to access some free services provided by CSP. The client VMs are managed by VMM in our case, we have proposed the use of KVM hypervisor running on a Linux Host OS. Since these VMs of un-trusted users are not trusted, they might be malicious and their target might be to threat the EO or the CSP. The proposed model is divided into two major parts for managing the security i.e. Management of security by CSP and client. CSP is responsible to secure all layers of computing infrastructure against outsider's attacks. Clients are responsible to secure and control their personal data against insider's attacks by acquiring a remote cryptography software using Security as a Service (SECaaS). The proposed model is developed by using several security tools as well as techniques such as SECaaS, TPM, vTPM, Virtual Firewall (VFs), Intrusion Detection Systems (IDS) and TVD to eliminate the threats of malicious VMs on the VMs of the EO and to block the insider to view or misuse the data of EO as shown in Fig.1. The detailed mechanism of our security model is further described.

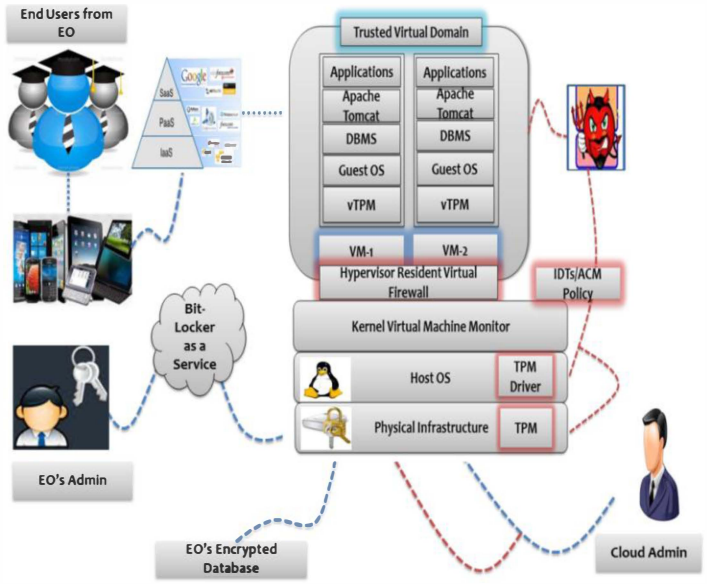

Figure 1. Efficient and Secure Educational Platform (E-SEP) on CCI

A. Securing the Virtualization Layer

We have proposed the use of IDTs, TVD, TPM driver, vTPM and hypervisors-resident VF to secure the virtualization layer that includes VMs and VMM. These tools will be illustrated as follows:

1) Intrusion Detections Tools (IDTs)

IDTs will collect and analyze data from a computing system, aiming to detect intrusive actions. We propose the use of two main approaches for IDTs i.e. Network-based IDTs (NIDTs) and Host-based IDTs (HIDTs), NIDTs will monitor the network traffic flowing through the systems whereas HIDTs will monitor the local activities on a host like processes, network connections, system calls, logs, etc and examining events like which files have been accessed and what applications have been executed [13].

2) Trusted Virtual Domains (TVDs)

Since isolation is one of the main solutions to eliminate the threat of malicious VMs attacking on VMs of trusted users. In our model, isolation is achieved by using the technique of TVD, which is formed at CCI by grouping the related VMs running on separate physical machine into a single network domain with a unified security policy. The multiple instances of TVDs co-exist on a single platform under a shared resource policy. The use of TVD provides strong isolation among un-related VMs as the communication among VMs will take places only according to the security policies configured by administrator in the VMM. A malicious VM cannot join any TVD because it should fulfil the access policy requirements so no any malicious VM will affect the VMs of trusted users on cloud [14]. Normally the VMs residing in a TVD are labeled with a unique identifier. The labeling is used to identify the assigned VMs to a particular customer and to allow the same labeled VMs to run inside the same TVD.

3) TPM Driver and vTPM

In order to protect the KVM hypervisor from attacks of malicious VM, we need to secure the OS kernel. To achieve this, we have proposed the use of TPM driver at this layer. It is a kernel-mode device driver designed for TPM, it will allow the host OS to communicate with hardware TPM that will provide more platform stability and eliminates the need for vendor-specific device drivers. TPM driver can be used in various OSs such as Windows and Linux to protect the OS from attacks [15]. If OS is free from attacks the security of hypervisor will remain alive. Since the physical TPM is used to protect the host OS and underlying physical platform and the use of vTPM, it provides same TPM like functionality for VMs, each VM will have its own vTPM instance that will be created by vTPM manager and will keep running throughout the lifetime of the VM which will communicate with underlying TPM through drivers. The use of vTPM will ensure the integrity and consistency of VMs'.

4) Hypervisor-Resident Virtual Firewall

Hypervisor-resident VF that is implemented on the VMM and it is responsible to capture malicious VM activities including packet injections. The VF requires a modification to the physical host hypervisor kernel to install process hooks or modules allowing the VF system access to VM information and direct access to the virtual network switches as well as virtualized network interfaces moving packet traffic between VMs. The hypervisor-resident VF can use the same hooks to then perform all firewall functions like packet inspection, dropping, and forwarding but without actually touching the virtual network at any point [16].

B. Securing the Physical Layer

Physical layer is secured by a TPM. Its implementation is available as a chip that is physically attached to a platform's motherboard and controlled by software running on the system using well-defined commands. It provides cryptographic operations such as asymmetric key generation, decryption, encryption, signing and migration of keys between TPMs, as well as random number generation and hashing [17]. TPM also provides secure storage for small amounts of information such as cryptographic keys. Because it is implemented in hardware and presents a carefully designed interface, TPM is resistant to software attacks [18]. Physical layer is secure proof mainly by TPM's Trusted Execution Technology (TXT). It is a feature of Intel's microprocessors and chipsets commonly referred to as Intel vPro. It provides a late launch capability for the secure creation and launch of virtual execution environments called Measured Launch Environments (MLEs) that can be launched anytime after a platform is booted. Hardware protections are provided by TXT against software based attacks on MLEs during launch and while the MLE is executing [6]. The use of MLEs will monitor the performance of computing infrastructure and block any possible threats by outsider attackers to underlying hardware.

C. Security as a Service / (Bit-Locker as a Service)

By acquiring SECaaS, administrator from an EO will be able to protect their particular data storage disks by performing cryptographic encryption and decryption operations. This target will be achieved by providing remote access of TPM enabled software i.e. Bit-Locker Drive Encryption as a service to the client. It is a new security feature that provides better data protection by encrypting all data stored on the OS volume. For-example if client's data is stored on drive "C", the CSP must enable the client to encrypt that particular drive via Bit-Locker as a Service. Once the client's admin activates Bit-Locker on their volume, a password will be required that will use a master or private key for the client and upon successful activation, a recovery file will be generated by the software, this file can be used in case of forgetting or losing the master key, the master key and recovery file must be only known to a highly privileged person from the EO such as administrator and should be stored on an isolated device not on the machine at which encryption has taken place. Once the data is sealed by the client the volume will be displayed with golden lock [18] as shown in Fig.1. However, Bit-Locker can only be used with TPM to perform the required tasks such as sealing and unsealing to protect the user's data. Under this mechanism of SECaaS, the clients will be confident that their data are protected from any insider threat at CSP side.

VII. Conclusion and Future Work

Cloud computing is considered as a key enabler to develop an EEP that will be used for supporting globalized and collaborative education. Current educational platform are cost-consuming, whereas an educational platform on CCI will be cost-effective in-terms of scalability, availability, on-demand self service, recovery and flexibility. However, there are certain barriers of security that are blocking the EOs from adopting cloud computing. In order to contribute in the field of cloud computing security, we have designed a conceptual security model to support the deployment of education platform on CCI. This model is based on analysis, concepts and theories. However we will focus on providing a practical prototype by implementing the proposed model in our upcoming research publication.

Acknowledgment

We are thankful to God Almighty for giving us the knowledge and wisdom to complete this work. We are also thankful to our parents for their encouraging support.

References

[1] UNESCO, 2010. Cloud Computing in Education, Available from http://iite.unesco.org/pics/publications/en/files/3214674.pdf.

[2] M. Erkoc, Kert, 2011. Cloud Computing for Distributed University Campus: A Prototype Suggestion, in International conference on the future of Education.

[3] Sultan Nabi, 2010. Cloud Computing for Education: A new dawn? In International Journal of Information Management: Elsevier, pp. 109-119.

[4] Filip A., Rolul, 2011. Stakeholderilor in teoria de marketing relational (The role of stakeholders in relationship marketing theory in Romanian), Calitatea – access la success Journal (Quality1access to success), no. 3, 2011, pp. 27130.

[5] S. Pearson and A. Benameur, 2010. Privacy, Security and Trust Issues Arising from Cloud Computing, in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference, pp. 693-702.

[6] F. John Krautheim, 2009. T Private virtual infrastructure for cloud computing, in TRUST'10 Proceedings of the 3rd international conference on Trust and trustworthy computing.

[7] Katz, R., et al., 2009. Demystifying Cloud Computing for Higher Education (Research Bulletin, Issue 19). Boulder, CO: EDUCAUSE Center for Applied Research, Available from http://www.educause.edu/ecar.

[8] Z. Yang, 2011. Study on an interoperable cloud framework for e-Education, In International Conference on E -Business and E-Government (ICEE), pp. 1-4.

[9] R. Elumalai, V. Ramachandran, A Cloud Model for Educational e-Content Sharing, In European Journal of Scientific Research, ISSN 1450-216X Vol.59 No.2 (2011), pp.200-207. Page 6 of 6 IEEE Security & Privacy.

[10] Sengmei Luo, et al., 2011. Virtualization security for cloud computing service, In International Conference on Cloud and Service Computing (CSC), vol., no., pp.174-179, 12-14.

[11] CSA, 2009. Security guidance for critical areas of focus in cloud computing V3.0, Available from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[12] Srinivasan, et al., 2012. State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud computing environment, In: International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012), ICACCI '12, ACM, 2012, Chennai, India.

[13] Harley Kozushko, 2003. Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[14] Luigi, C., et al. Trusted Virtual Domains – Design, Implementation and Lessons Learned, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[15] Microsoft, 2007. TPM Driver, Available from http://technet.microsoft.com/en-us/library/cc734122(v=ws.10).aspx.

[16] Clement Berthelot, 2011. Evaluation of a Virtual Firewall in a Cloud Environment, Available from http://buchananweb.co.uk/09014406_MSc_VirtualFirewall.pdf.

[17] Common Criteria. Trusted Computing Group (TCG) Personal Computer (PC) Specific Trusted Building Block (TBB) Protection Profile and TCG PC Specific TBB With Maintenance Protection Profile, July 2004.

[18] Microsoft, 2012. Trusted Platform Module Administration Technical Overview, Available from http://technet.microsoft.com/enus/library/cc766159(v=ws.10).aspx