Designing a Trustable Security Protocol for Implementing a Smart Educational Platform on Cloud Infrastructure

Sarfraz Nawaz Brohi
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
sarfraz_brohi@hotmail.com

Mervat Adib Bamiah
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
mervatbamiah@yahoo.com

Suriayati Chuprat
Advanced Informatics School
Universiti Teknologi Malaysia
Kuala Lumpur, Malaysia
scsuria@gmail.com

Abstract— **Due to revolutionizing growth of technology, globe is transforming from the traditional to smarter aspects of leading life. Smarter life refers to an aspect of life that is completely dependent on the use of smart digitalized technology (smart phones, iPods, sensors, intelligent microchips and robots) to gain rapid development with high success factor. In order to achieve the target of enabling smarter and healthy life we require smart youth leaders. The smart young generation will be created by developing smart educational systems that are running on a smart educational platform. Cloud computing is considered as a smart business model for providing a smart educational platform by enabling the integration between heterogeneous organizational processes. Since cloud computing is open access global technology where organizations data and applications are residing on the cloud, there are numerous probabilities of security threats. Organizations feel lack of control on their confidential data which impacts the trust of adopting this technology that actually results into a major obstacle of developing a smart educational platform. In this research paper, we describe the significance of smart educational platform and propose a cloud computing security model for developing a smart and secure and ubiquitous educational platform.**

Keywords- Smart Education; Cloud Computing; Virtualization; Security Threats

I. INTRODUCTION

Education is a fundamental element in every country's development and building strong economy for a long term successful future and consequently smart education could be considered the most effective, reliable and modern method in personal and organizational development. A smarter education system can empower the educational associated entities such as administrative staff, management and teachers to develop a workforce with high value and global skills [1]. World is globalized but unfortunately our educational system is still individualized where students are bound to a close room lectures and accessing the university specific resources by using relevant internet sites and private university systems, this learning approach normally narrows the students' innovation in today's competitive era of business and IT. Individualized educational system not only creates the problem for students but also for the lecturer's. They are overburdened with the administrative task such as marking the attendance for students, preparing worksheets and marking students' exams. Globalization and technology advances are rapidly changing skill requirements. Tomorrow's graduates will primarily be employed as knowledge workers in country's services-based economy [2]. They must have skills to succeed in this challenging work environment. There is need to transform the educational systems to a globalized smart educational platform that is consist of three factors interconnection, instrumentation and intelligence. Interconnection refers to the integration and sharing of heterogeneous technological resources. Instrumentation will enable the entities to gather data from various sources across the educational glob and intelligence will enable the entities to make decisions that will improve the learning process [3]. This research paper is structured into six sections. Section-II describes the significance of smart educational platform. Section-III describes the role of cloud computing in developing a smart educational platform. Section-IV describes the issues that create a barrier to develop smart educational platform. Section-V critically appraises the related work in the research area of smart education and cloud computing. Section-VI illustrates the overall explanation of proposed security technique/protocol to design a smart educational platform on cloud. Finally Section-VI represents the overall conclusion and future direction of undertaken research.

II. FOUR SIGNS FOR TRANSFORMING FROM TRADITIONAL TO A SMART EDUCATIONAL PLATFORM

Traditional educational systems respond are facing the challenges of limited resources, inflexible infrastructures, entrenched processes, increasingly incoherent and

incompatible data and rising consumer demands [4]. Current structure of educational process is not efficient enough. There are four major visible signposts that indicate us to move from traditional to smart educational platform. The signposts are described as follows:

A. Rapid Emergence of Internet and Digital Devices

Due to revolutionized used of internet and rapid development in the field of information technology, modern generation of students are addicted to use of latest digital devices for completing their normal everyday tasks such as information sharing, conferencing, e-learning and socializing. Young people have come to depend on digital resources for communications, learning and entertainment activities at home, school or workplace. This category of modern internet students is different from the traditional students who were relying on pen, paper, letters and other physical tools for communication, collaboration and learning. The 21st century students are at ease with technology and easily adapt and integrate new functionality from smart phones, laptop computers, mp3 players, game stations, and virtual reality worlds [4]. They arrive at school expecting to leverage technology in the learning environment just as they do in their personal lives. Unfortunately, our current educational platform is not upgraded to support the desired demands of students.

B. Competitive Industry Requirements

Considering the upcoming business demands and challenges, industries are looking forward to build competitive work force by hiring employees with highly upgraded and innovative skills. The requirements of industries have created a tough completion among the young generation. Employers increasingly hire workers who possess both job-related skills and foundational competencies that indicate an individual's potential to adapt to changing market and economic circumstances. Educational industries are responsible to produce competitive students by reshaping the traditional education system into interactive method and by creating students with professional academic as well as industrial working skills to satisfy industrial requirements. The employees of tomorrow need to solve the problem one they have never solved previously [4]. The work requirements no more remain as redundant and repetitive tasks because the sun of every day is rising up with a new challenge from business organizations.

C. E-education and Green Environment

Electronic education or so called remote education is growing faster due to its flexibility of leaning environment and time constraint. Educational offerings are no longer constrained by physical place and time. Students and parents are free to choose from a wide variety of primary and supplementary remote educational service providers that complement their needs, abilities, means and preferences. Transformation from traditional to smart online education partially or fully has huge impact on cutting material costs such as papers that also keeps the environment green as the elimination of cutting millions of trees to manufacture papers. In addition to removing the burden of carrying heavy bags full of books and making the education system more intelligent, enjoyable, pervasive and ubiquities, let alone reaching unlimited number of users from different categories such as normal, disabled, young, old, employee, trainer, administrator in multiple organizations or individually [4].

D. Global Integration

Advancements in technology have eliminated traditional lines that defined the boundaries of an educational institution. Global integration has raised the awareness of the potential for improved outcomes with greater personalization and productivity allowed new service providers to enter well established educational markets, introduced opportunities for institutions to extend their linkages to new populations of youth and adult learners. With these new models for teaching and learning, education is confronted by the fourth signpost. How does an educational institution participate in a globally integrated world? A globally integrated world will create opportunities for institutions to reach new learners, for learners to access new resources, and as a result, create a more integrated web of collaborators and resources [4]. While this leads to more competition, it also means greater need for collaboration skills among the workers of tomorrow, greater ability to access and manage information, and greater cultural awareness.

III. CLOUD COMPUTING: A KEY ENABLER TO DEVELOP A SMART EDUCATIONAL PLATFORM

Traditional educational systems are dependent on organization's platform and the academic tasks are carried out by relying on local university individual systems. Consider a private or public university where some processes (marking student's attendance, submission of assignments, submitting lecture material, preparing students results) are being carried on the systems that have limited accessibility features. In other words these systems can be accessible via only limited devices at limited time and location.

These traditional systems should move to a smart educational platform that is flexible and ubiquitous in nature. Users of the system should be facilitated to access the resources or application at any time, from any location by using any smart digital device. To achieve these requirements, it's good to implement smart educational platform on a cloud computing architecture that is globally accessed and flexible to support heterogeneous requirements of smart education system. Due to the flexible features of cloud computing, it can be a great support to transform traditional education into a smart education. Cloud computing is not only valuable to be used in educational organization but in almost every business organizations. Looking at the feature trend and current facilities of cloud computing, we can say that cloud computing can be backbone of smart education system [5]. Cloud computing is available to access from any location, at any time by using a smart device such as notebook, tablet, iPods or

smart mobile phones [6]. Due to ease of accessibility it removes the burden on several entities involved in using education systems such as students and lecturers. For-example students can mark their attendance by using personal card readers or biometric device and they can submit their homework on cloud by using any device at any time. On the other handle lecturers can also easily access the records of students and submit their work progress on cloud that can be accessed by administrative staff to view and monitor the students' academic progress. The central access of cloud computing can enable the entities to focus on their actual tasks rather than getting busy in overloaded unnecessary tasks. Unfortunately due to security and trust issues in cloud computing educational organizations are not ready to move to cloud, that creates a major obstacle to create a smart educational platform. In this research paper we will design a security technique to overcome issues of security and trust on adopting the paradigm of cloud computing.

IV. Barriers in Adopting Cloud Computing for Developing Smart Educational Platform

Beside the advantages of cloud computing it should be also considered that sometimes cloud can be rainy as well. In other words cloud is an open access platform so security on cloud is not trustworthy. When data of a client is on the datacenter of third party cloud provider, there are obvious chances of security, hack, theft and malicious activities that can be performed by illegal users such as hackers. Cloud computing datacenter environment is overloaded with trust issues [7]. The client must not only trust the datacenter operator/provider, but each of individual clients that are collocated in the facility and each third party service provider of the operator. Clients needs assurance that their sensitive information is protected from compromise and loss and that their application is available when demanded [17] [9].

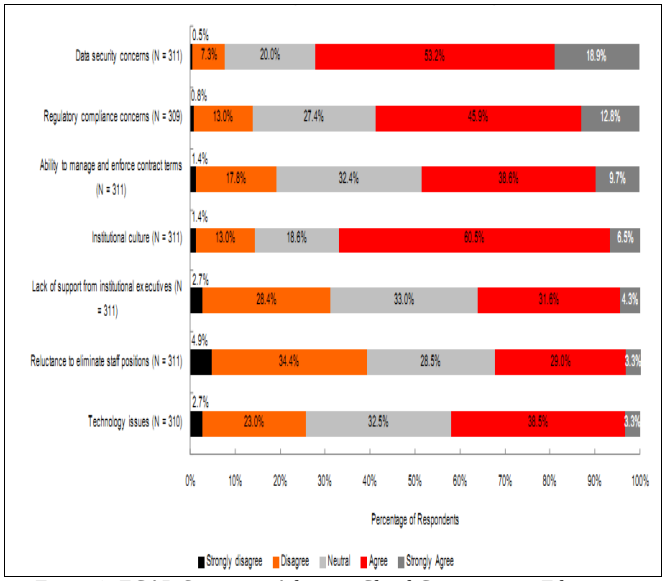

Figure 1- ECAR Survey on Adopting Cloud Computing in Education

In a survey conducted by ECAR as shown in figure-1, 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 will limit their adoption of these emerging service offerings [11].

No suspect that cloud computing can be key enabler for a fundamental to transformation from traditional educational platform to a smarter education platform, but survey results clearly shows that educational organization believe security is their main concern for not moving towards cloud. Since security is a vital factor for organizations policies, the education organization need to be guaranteed on security provided before adopting the services on cloud. The security challenge is faced in cloud computing due to two main potential issues. First issue is threats of attack on client VMs [8] on cloud and second issue is lack of data governance [10] of clients to control the security of their personal data. Both issues are described in great detailed as follows.

A. Malicious Virtual Machine Attack

In a virtualized cloud computing platform, the VMs of clients that are running client specific applications are residing on a virtualization layer [12]. Due to weak isolation techniques, virtualization is prone to bugs and vulnerabilities that a malicious virtual machine (VM) [13] an exploit to attack or obstruct other VMs if any of the VMs is malicious or affected with virus [17] it would have to capability to compromise and threaten all the remaining clients in the datacenter [8] destroying the trust and integrity of all parties involved [17] as shown in figure-2 [8].

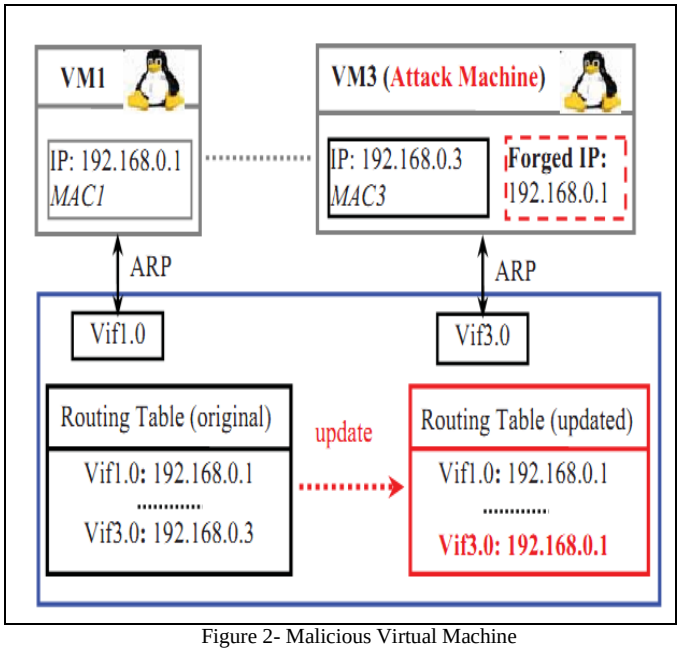

Figure 2- Malicious Virtual Machine

However, there are various VMM techniques available to address this gap but even these hypervisors techniques have exhibited flaws [13] that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. There is need of a strong isolated technique that should ensure that VMs individual customers don't impact the operations of other tenants running on the infrastructure of same cloud provider.

B. Data Governance / Trust Issue

Securing the virtual layer is not sufficient enough to satisfy the education organizations to adopt cloud computing. In order to satisfy the clients to trust this technology security must be extra matured. Since data is stored on the cloud with the provider, the maintaining the security of VM is fully under the responsibility of cloud provider so clients do not feel sense of control on their personal data, in the result clients such educational organizations where privacy is vital act, don't fully trust on the provider [10] so they don't adopt cloud computing. If security control is somehow under the control of clients for-example if security control is shared between client and provider, client will be satisfied enough to move their data on cloud due top personal control on their personal data. In order to deeply clarify this particular issue in the cloud computing, consider an example of an owner of shopping mall and tenants. For-example a shopping mall is given to the tenants on rental, where they are required to pay according to the usage of resources such as rental for the shop, but security and maintenance will be provided by the owner. Tenants are not responsible about security and maintenance so it saves cost and time for them. On the other hand, security keys are only with the owner. When tenants are saving all their personal resources inside the shopping mall of a third party owner, the issue is that how to trust that their resources will be safe without any security threats. Now applying the same scenario on cloud computing, suppose the owner of the mall is the cloud provider such as Google, Amazon or Microsoft and tenants are the education organizations. The clients will use the datacenters of cloud provider and if security is under the management of cloud provider, clients are not confident enough to trust the provider because their information is very critical, so it is a challenging task to provide trust to the clients where information is very critical.

V. Related Work

(Z. Yang, 2011) [22], suggested framework an open structure framework, can interoperate with external content and social service, it can also interoperate with enterprise apps (such as CRM, ERP, Groupware, SharePoint, etc) and consumer apps (such as twitter, g-mail, YouTube, etc) at the data level by mapping mechanism. It has four layers i.e. user experience, collaboration service, core service, and delivery platforms. This framework can make internal cloud and the 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) [23] 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 few personal information like their email Id, geographical position, mobile number along with a request to identify them as user or content provider. Once they have entered the requested details, a unique One Time Password (OTP) is dynamically generated and is sent to their mobile number and to the email Id which can be used for confirming the 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.

VI. Our Contribution: Smart and Secure Educational Platform on Cloud

To address the issues (malicious VM attack and data governance) discussed in section-III, we have designed a trustable security protocol. The protocol consists mainly on two parts management of security by provider and management of security by client. The provider is responsible to secure all the layers of computing infrastructure from outside attacks such as malicious VM attack and client is responsible to secure and control their personal data by acquiring a service we termed, Security as a Share Agreement (SaaSA) from the provider. When education systems are transferred to a cloud infrastructure, the organization applications will be running on VMs and data will be stored on physical storage. In this case cloud infrastructure will have three layers i.e. Application, Virtualization and Physical as shown in figure-3. The designed protocol is used to secure each layer of the infrastructure and provides the ability to clients for governing their data. The following section will describe the overall technique of protocol at each layer of computing infrastructure.

A. Application Layer

At this layer client applications are running on the VMs. In this model, we have suggested the use of Moodle as SaaS to education organizations. Moodle is an Open Source Course Management System (CMS), also known as a Learning Management System (LMS) or a Virtual Learning Environment (VLE). Many institutions use it as their platform to conduct fully online courses, while some use it simply to augment face-to-face courses known as blended learning. Many other users use its activity modules such as (forums, databases and wikis) to build richly collaborative communities of learning around their subject matter in the social constructionist tradition that provides the essence of globalised education. On the other hand Moodle can be also used to deliver content to students such as standard packages and assess learning using assignments or quizzes [14] that help to

remove the burden of carrying out manual and time consuming tasks. Since in our suggested model, Moodle is running on a cloud platform, due to ubiquitous and pensiveness nature of cloud computing, Moodle can be accessed by thousands of users from any location at any time by using any smart digital device such as smart phones, iPods, tablets, notebook etc.

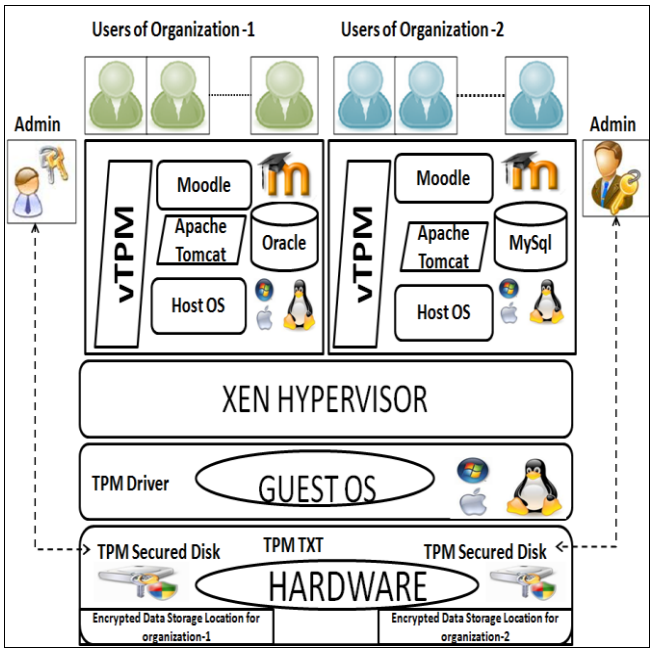

Figure 3- Smart and Secure Educational Platform on Cloud

Strong security is provided at application layer by using vTPM instances on each VM on cloud. A vTPM instance is the virtual form of TPM used at VM. It is supposed to implement the full TCG TPM Specification version 1.2. Each VM has its associated vTPM instance running throughout the lifetime of the VM, so there as much vTPM instances as there is VMs running. A vTPM instance associated to a VM is unique. The vTPM implementation in Xen is software-based, so a vTPM instance is just a piece of software running on a VM [15]. Due to use of vTPM, applications are accessed only by the authorized users such as university staff, students, and administration. No any authorized or malicious client can target or access the VM of university because it is secured by a vTPM instance that requires full privilege access and authorities to access the resources running on a VM.

B. Virtualization Layer

The VMs acquired by education organizations are managed by using Virtual Machine Monitor VMM [8], also known as hypervisor. It allows multiple operating systems to simultaneously run on one machine. A VMM is a software layer that meets two basic requirements, it provides a VM abstraction that models and emulates a physical machine and it provides isolation between virtual machines. The basic responsibility of a VMM is to provide CPU time, memory and interrupts to each VM. If security of hypervisor is compromised, the malicious user will create unlimited number of VMs to disturb the performance of computing platform. In order to secure the VMs on cloud, the underlying physical layer must be strictly secured so that attacks don't break the security of architecture. There must be complete chain of trust from the security of hardware to the virtual layer where VMs are running. At virtualization layer, we assume that there are two VMs that are running the Learning Management System for two universities. The VMs are managed by using Xen hypervisor. Xen hypervisor is running directly on the underlying OS [13]. To protect the Xen hypervisor from attacks we need to secure the OS kernel. To achieve this sense of security we have proposed the use of TPM driver at this layer. The TPM driver is a kernel-mode device driver designed for TPM security hardware that conforms to the Trusted Computing Group (TCG) 1.2 specifications. Conforming to TCG 1.2 provides more platform stability and eliminates the need for vendor-specific device drivers. TPM driver is used in various OS systems such as Windows and Linux to protect the OS from attacks [18]. If OS is free from attacks the security of hypervisor will remain alive.

C. Physical Layer

This layer involves the use of physical devices such as storage and processing units. This layer is the first component to be secured in any trusting computing infrastructure. In our architecture physical layer is secured by a TPM. The TPM is a security specification defined by the Trusted Computing Group [19]. Its implementation is available as a chip that is physically attached to a platform's motherboard and controlled by software running on the system [16] using well-defined commands [20]. 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. It also provides secure storage for small amounts of information such as cryptographic keys. Because the TPM is implemented in hardware and presents a carefully designed interface, it is resistant to software attacks [21]. The 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 [17]. TXT provides a late launch capability for the secure creation and launch of virtual execution environments called Measured Launch Environments (MLEs). MLEs 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 [17]. The use of MLEs will monitor the performance of computing infrastructure and block any possible threats to underlying hardware.

D. Security as a Shared Agreement-SaaSA

The smart education model on cloud shown in figure-3 represents that each layer is secure by using a TPM enabled technique, but as we discussed previously this not enough to satisfy the client to adopt cloud computing because clients are not aware and fully trusting the security technique used by the

provider when their data is on open access cloud computing platform. They believe even if their data is protected from outsider's attack but what about the trust on provider. It's possible that provider or malicious employee of provider may view and misuse their organizations confidential data. In order to remove this issue of trust on provider, we have proposed the use of shared security agreement between education organizations and cloud provider. The all three layer will be secured by provider to protect the platform from illegal attacks but client confidential data will be under the security managed by a technical administrator from education organization. So security will act as a shared agreement between educational organizations and cloud provider. By utilizing SaaSA, the administrator from an education organization will be able to protect the particular storage disks on which their data is stored. This target will be achieved by using TPM enabled software called as BitLocker.

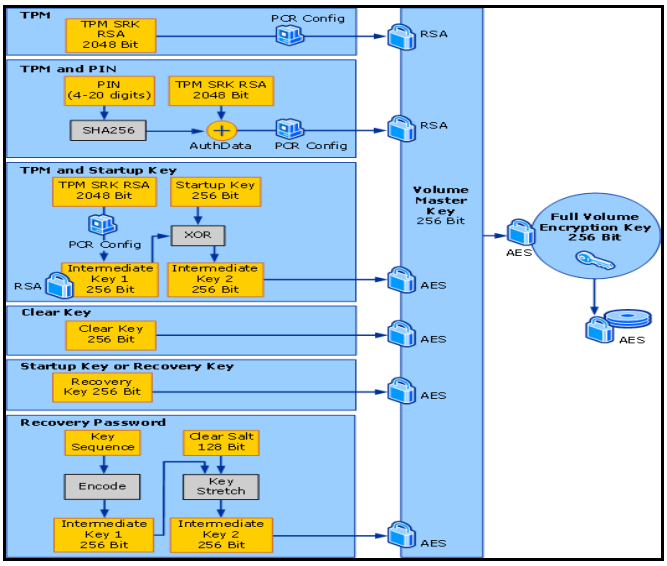

Figure 4- BitLocker and TPM Master Key Generation

BitLocker Drive Encryption is a new security feature that provides better data protection for the data, by encrypting all data stored on the OS volume. A volume may consist of one or more partitions on one or more hard disks. BitLocker works with simple volumes, where one volume is one partition. A volume usually has a drive letter assigned, such as "C". BitLocker works with a TPM supported system means the underlying provider's system must have a TPM as shown in the proposed model. TPM is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft [18]. BitLocker uses the TPM to help protect the OS and user data. Using the BitLocker-protected the data containing volume of client is encrypted with a full volume encryption key, which in turn is encrypted with a volume master key. Securing the volume master key is an indirect way of protecting data on the volume [19]. Figure-4 shows the process of BitLocker generating a master key by using TPM.

Once BitLocker authenticates access to the protected operating system volume, a filter driver in the OS file system stack encrypts and decrypts disk sectors transparently as data is written to and read from the protected volume. When the computer hibernates, the hibernation file is saved encrypted to the protected volume. When the computer resumes from hibernation, the encrypted hibernation file is decrypted [19].

Under the technique of SaaSA, when data of client is encrypted by using BitLocker, the master encryption keys are only visible to the client. In this case a personal such as only admin from education organization can view or modify the data. In this case even a provider is not allowed to access the organizations private data. When organizations are able to control the security of their own data, they will feel satisfied enough to adopt the paradigm and services of cloud computing which in result will help us to formulate smart and secure educational platform which supports for performing automated tasks, ubiquitous access and globalised education for the global world.

VII. Conclusion And Future Work

Cloud computing is considered as a key enabler to develop smart educational platform that will be used for supporting globalized and collaborative education. There are certain barriers that are avoiding education organizations to adopt the paradigm of cloud computing. Security is one of the top concerns that has been obstacle between educational organizations and cloud computing. In order to contribute in the field of cloud computing security, we have designed a security model to support the deployment of education systems on cloud. The model represents the use of VMs that are running learning management systems i.e. Moodle at the application layer. VMs are managed by Xen hypervisor that is running on host OS. The proposed model is secured by using TPM security technique at each layer of computing platform i.e. physical, virtualization and application layer. In order to provide full trust, we have suggested the technique of SaaSA, where client is able to manage their own security as a shared agreement. The techniques designed in this research paper will be implemented in the future work on a cloud platform. This research can be considered as a piece of contribution for improving the security of cloud infrastructure to deploy develop smart educational platform. However, there are still tremendous opportunities for industry and academia researchers to contribute in this area of research.

Acknowledgment

We are thankful to Almighty Allah for giving us the courage, knowledge, patience and health to complete this work. Secondly we are dedicating credit of accomplishing this research paper to our parents for their moral support. We are also thankful to our supervisor for always being flexible with us. Finally we are thankful to UTM AIS for providing us the platform of PARIS to publish our research paper.

REFERENCES

[1] Salimia L., Ghonoodib A., 2011, The study and comparison of curriculum in smart and traditional schools, WCES12011 World Conference on *Educational Sciences 2011, Procedia1Social and Behavioral Sciences*, ISSN: 187710428.

[2] The Cisco Connected Insight Series. Thought1 provoking discussions on common issues facing public sector agencies today in government, education, healthcare, and safety and security. *Transforming Education,Transforming Lives: A Path Toward Next Generation Learning*, DRMKT/LW16083, 2009.

[3] Lorena Batagan, Catalin Boja., 2011, Smart Educational Systems and Education Clusters, *International Journal of education and information technologies*. Issue 4, Volume 5.

[4] IBM, 2009. Education for a Smarter Planet: The Future of Learninghttp://www.ibm.com/smarterplanet/global/files/dk__da_dk__education__the_future_of_learning.pdf.

[5] Bo Wang and HongYu Xing, "The application of cloud computing in education informatization," *in Computer Science and Service System (CSSS)*, 2011 International Conference on, 2011, pp. 2673-2676.

[6] T. A. Henzinger, A. V. Singh, V. Singh, T. Wies, and D. Zufferey, "FlexPRICE: Flexible Provisioning of Resources *in a Cloud Environment," in Cloud Computing (CLOUD)*, 2010 IEEE 3rd International Conference on, 2010, pp. 83-90.

[7] Filip A., 2011. Rolul stakeholderilor in teoria de marketing relational (The role of stakeholders in relationship marketing theory in Romanian), *Calitatea – acces la succes Journal (Quality1access to success)*, no. 3, 2011, pp. 27130, ISSN 158212559.

[8] Hanqian Wu, Yi Ding, C. Winer, and Li Yao, "Network security for virtual machine in cloud computing," in *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, 2010, pp. 18-21.

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

[10] Zhiyun Guo, Meina Song, and Junde Song, "A Governance Model for Cloud Computing," in *Management and Service Science (MASS)*, 2010 International Conference on, 2010, pp. 1-6.

[11] Katz, Richard N., Philip J. Goldstein, and Ronald Yanosky. "Demystifying Cloud Computing for Higher Education" (Research Bulletin, Issue 19). Boulder, CO: EDUCAUSE Center for Applied Research, 2009, available at http://www.educause.edu/ecar.

[12] Hanfei Dong, Qinfen Hao, Tiegang Zhang, and Bing Zhang, "Formal Discussion on Relationship between Virtualization and Cloud Computing," in *Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2010 International Conference on*, 2010, pp. 448-453.

[13] Bharadwaja, Weiqing Sun, M. Niamat, and Fangyang Shen, "Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System," in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, 2011, pp. 695-700.

[14] Moodle, 2011. What is Moodle, available at http://moodle.org/about.

[15] Thomas J, 2006. vTPM: Virtualizing the Trusted Platform Module: IBM Research Report, available at http://domino.research.ibm.com/library/cyberdig.nsf/papers/A0163FFF5B1A61FE85257178004EEE39/$File/rc23879.pdf.

[16] Trusted Computing Group, 2005. TCG TPM specification Version 1.2-Part 3 Commands, 2005.

[17] F. John Krautheim, "T Private virtual infrastructure for cloud computing", *in TRUST'10 Proceedings of the 3rd international conference on Trust and trustworthy computing*, 2009, ISBN:3-642-13868-3 978-3-642-13868-3.

[18] Microsoft, How does BitLocker Drive Encryption work? available at http://windows.microsoft.com/en-MY/windows-vista/BitLocker Drive-Encryption-Overview.

[19] Microsoft Technet, 2009. BitLocker Drive Encryption available at http://technet.microsoft.com/en-us/library/cc732774(WS.10).aspx.

[20] Trusted Computing Group, 2011. available at http://www.trustedcomputinggroup.org.

[21] 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.

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

[23] 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.