Analysis of Virtual Machine Migration Security Architectures in Cloud Computing

Sam Njuki*, Jianbiao Zhang*and Edna Too*

College of Computer Science and Technology,

Beijing University of Technology

*College of Computer Science and Technology,
Beijing University of Technology

Abstract -- Migration in cloud computing allows the transfer of resources, such as Virtual Machine (VM) and data items from one cloud server to another cloud server. VM migration provides workload balancing and system maintenance features in the Cloud. Cloud service providers store VM disk images in encrypted form while at rest to prevent attacks. However, there is still the unresolved issue on how to ensure that data is moved securely to the cloud (VMs) and/or between clouds (VMs).The concern of this paper is to explore the security challenges that occur during cloud migration and come up with a better architecture to mitigate the security challenges posed during migration.In this paper, we analyze different cloud migration security models that have been proposed in relation to the security requirements during migration and report the strengths and weaknesses of each. To overcome the security challenges during cloud migration we report a better architectural model.

Key words -- Cloud computing, Cloud migration, Cloud Security Architecture, Virtual Machines (VMs),Virtual Machine Migration, Trusted Platform Module(TPM), Virtual Trusted Platform Module (vTPM).

1 INTRODUCTION

Cloud computing is a computing model in which software, hardware, infrastructure and platform are well defined and provided as a service [1]. Cloud computing is emerging from recent advancement in technologies such as GPU services, hardware virtualization, Web services, utility computing, distributed computing and automation of system.

Cloud computing make use of hardware virtualization technique to secure and allocate physical resources dynamically such as storage, computational power and networks to the users. Cloud resources are delivered to the end-users and customers through Web services.

The four main participants in a cloud architecture include: Cloud Provider, Cloud service owner,Cloud Consumer, Cloud Broker and Cloud Auditor [2].

There are three main layered categories provided by cloud providers. Each layer provides services to the layer above it. The first layer is Infrastructure as a Service (IaaS), followed by Platform as a Service (PaaS) and as the second layer and lastwe have Software as a Service (SaaS) [3].

Clouds can be categorized into five categories with respect to deployment model and isolation levels: Public Cloud, Private Cloud, Virtual Private Clouds, the Community Clouds and the Hybrid Clouds [4-10].

The fundamental concept of cloud computing is hardware virtualization, which is used to separate a single physical machine into several virtual machines (VMs) in a less costly way. In virtualization, several VMs can execute on the same physical machine. It's a cost-effective measure as several cloud consumers can lease the server resources. The same VMs can also be moved from one physical server to another physical server without so much delay. New VMs can be created easily and yet another benefit of virtualization is the VM location in the data center, which is regardless of the location and the ease of copying them [11,17].

Virtualizing the TPM is necessary to make its capabilities available to all virtual machines running on a platform. A virtualization where even though there may be more virtual machines in the physical TPMs, each VM is made to feel it has access to its own TPM when it needs it. [11]

Cloud providers are massive users of virtualization. However, there are risks posed by both physical machines as well as virtual machines server hosts and the guests. The four main types of virtual machine risks that can occur such as server host only, guest to guest, host to guest, and guest to host. Most risk models do not take care of them adequately [9]. Some of the risks occur during:1) ***Resource Allocation:*** When a physical memory, is allocated to a VM, the VM can use it for storing its data. If the resources are later transferred to another VMwhen it is not required anymore and therefore removed, the new VM could read the data from hard drive or memory. The data on such resources should be properly removed when being transitioned from one VM to the next.2)***Virtual Machine Attacks*:**If an

attacker successful gains access to one VM by exploiting a vulnerability in one of the applications running in that VM, he can attack other applications running in different VMs over the network. If the VM is running on the same physical host as the compromised VM, it may be hard to detect such network attacks. Therefore, there is need to monitor the traffic coming to and from each VM on the same physical host. 3)***The Hypervisor: The*** hypervisor or virtual machine monitor (VMM) is used to separate operating systems of VMs from the physical hardware. When a new VM is added on top of the same physical machine, it is vital to ensure that the operating system has been installed with the latest security updates and the software has been properly fixed. When an invader gains administrative rights to theguest operating system, he can go ahead and exploit the security weaknesses that exist in a hypervisor. By successfully exploiting such a security weakness, the invader can gain total access to the host physical machine. Furthermore, once the attacker has access to the host hypervisor, he can easily access all the VMs running on that physical machine.

Cloud migration allows transfer ofresources such as application, and data items from one cloud server to another cloud server or from an organization network computer to the clouds [12].

There are several benefits of cloud migration which includes Unlimited Scalability, Reduction of cost, capacity is increased, Automation, Flexibility and Better mobility [13].

The main challenge of cloud migration is cloud security. Therefore, special care needs to be taken at the time data is in transit to the cloud or migrated from one cloud server to another. As the organization is migrating business to the cloud, it has to move sensitive data from its computers or private networks to the cloud. In this transition, the organization has to think about the security solutions of this sensitive data.

The concern of this paper is to explore the security challenges that occur during cloud migration and come up with a better Architecture to mitigate the challenges posed during migration.

2 MATERIALS AND METHODS

2.1 Trusted Computing

Trusted computing provides a strongground on which to build a secure cloud. A Trusted Cloud Computing Platform uses a trusted component to provide a foundation for trust for software processes. The trusted computing specification [22] states that trusted platforms have two roots of trust, a Root of Trust for Measurement (RTM) which provides a secure measurement of the platform and a Root of Trust for Reporting (RTR) that allows certified report of measurement through attestation [3].

2.1.1 Working of Trusted Platform Module

The TPM [13] is the cryptographic component of the Trusted computing platform that serves as the RTR. TPM protects the encryption keys and other information by providing a storage Root Key(SRK).

Other important features include a *Non-Volatile Random Access Memory (NVRAM)*for safe storage of keys and user data and a random number generator for the key.

To determine if the TPM is genuine there is an*Endorsement Key (EK)*together with Endorsement Key certificate which provides a unique identification of the TPM.

An*Attestation Identity Key (AIK)*, signed by a privacy Certificate of Authority(CA), can also be created that is used to verify that the TPM is genuine; however, an AIK has no information that is distinctively identified to a single platform.

2.2 Virtual TPM Architecture

One problem associated with the TPM is that it works only for non-virtualized environments.

The TPM has a limitation in that it can be owned by only one entity at a time because TPM implantations specifications follow a one-to-one kind of relationship between the operating system and trusted platform.

Each guest needs to have full TPM functionality which is provided by virtualizing the TPM in the case where the platform is virtualized.

For this reason, specifications have been developed for a Virtual TPM (VTPM) [18] to provide the TPM functions for each virtual environment on the platform.

There exists a number of vTPM architectures which uses different methodology to virtualize the TPM.

2.3 Virtual Machine (VM) Operations

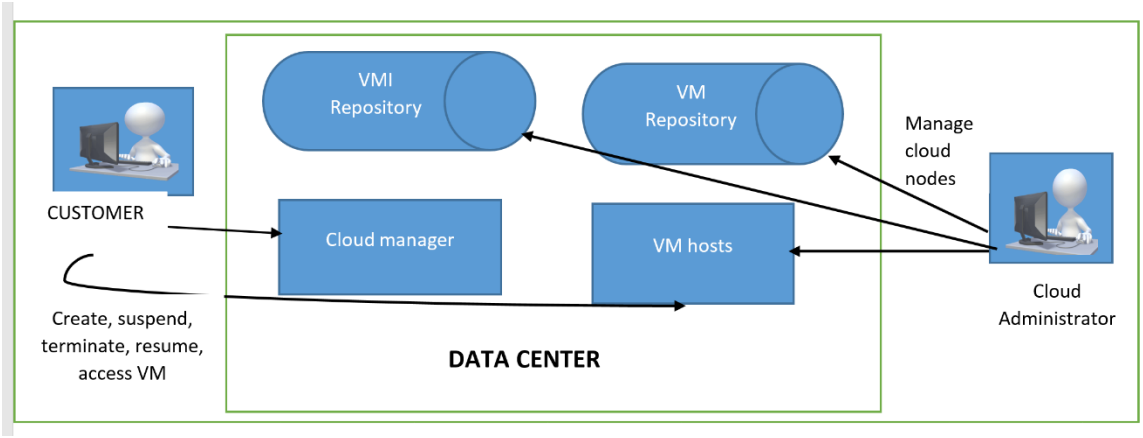

Figure 1: Abstract architecture of a typical VM hosting cloud service [14].

Figure 1 illustrates the architecture of a VM hosting cloud service. The services are hosted in several nodes. The guest VMs are hosted in the nodes under virtual Machine monitor (VMM). VMM is responsible for memory, CPU, disk scheduling, network management and security management of each VM.

The cloud manager coordinates the customer VMs by managing customer's IDs, additionally, it serves the requests of its customers for instance creation, termination, suspension of VMs.

Each VMI repository features different software configurations.

The VM repository stores the running states of the VMs e.g. creation, termination, resumption, access and Migration. It also enables the administrator to migrate customers VMs across cloud nodes for the sake of load balancing.

To perform VM migration the administrator instructs the cloud manager by indicating the target VM and destination cloud node.

The cloud manager interacts with the source and destination VMMs. The VMMs is responsible for initiating a VM migration protocol for transferring the state of VMs between nodes. Once it is done the VMM sends and acknowledgement message.

2.4 Related work

2.4.1 A Trusted Architecture for Virtual Machines on Cloud Servers with Trusted Platform Module and Certificate Authority

Yu Z., et al in their paper [14], combined the trusted computing and cloud computing security, to establish a trust system with a certificate authority (CA) and TPM as depicted in Figure 2. Their model can be used for VM and user authentication mechanism. Their experimental results show that trusted access mechanism can minimize communication overhead and reduce the time of issuing load certificates by applying for them offline.

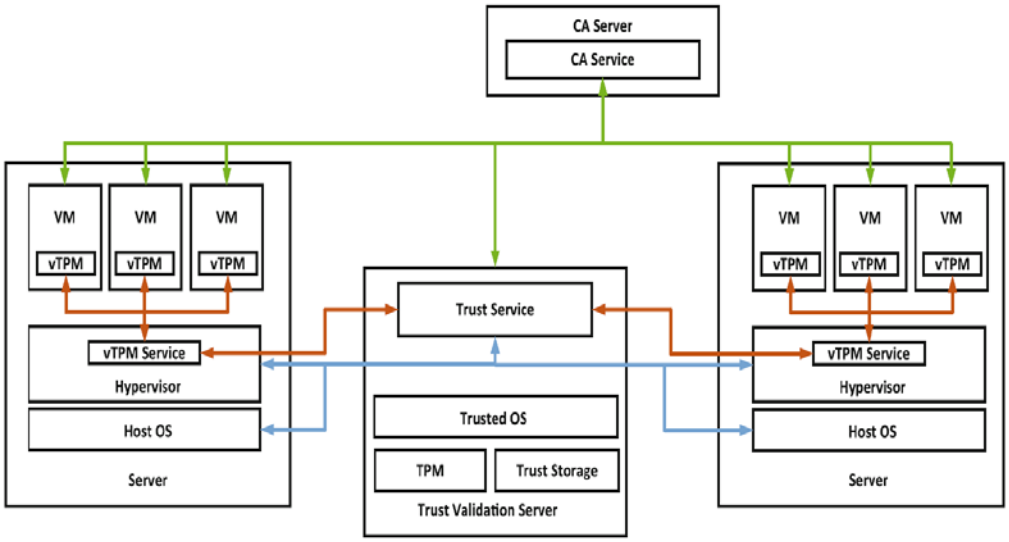

Figure 2: A trusted architecture of a virtual machine on cloud servers with TPM and CA as proposed by Yu Z., et al. in their paper [14].

2.4.2 Integrated Security for Services Hosted in Virtual Environments

Jayarathna D. et al. [15], In their paper, introduced a security architecture that combines TPM with hypervisor level access control and intrusion detection system. Their architecture provides anall-inclusivemethod for securing services hosted in VMs. Their architecture can also be applied in cloud computing security as well in distributed environments as shown in Figure 3.Additionally, their architecture is able to dynamically perform intrusion detection and update the security policies to protect the services from the identified threats.

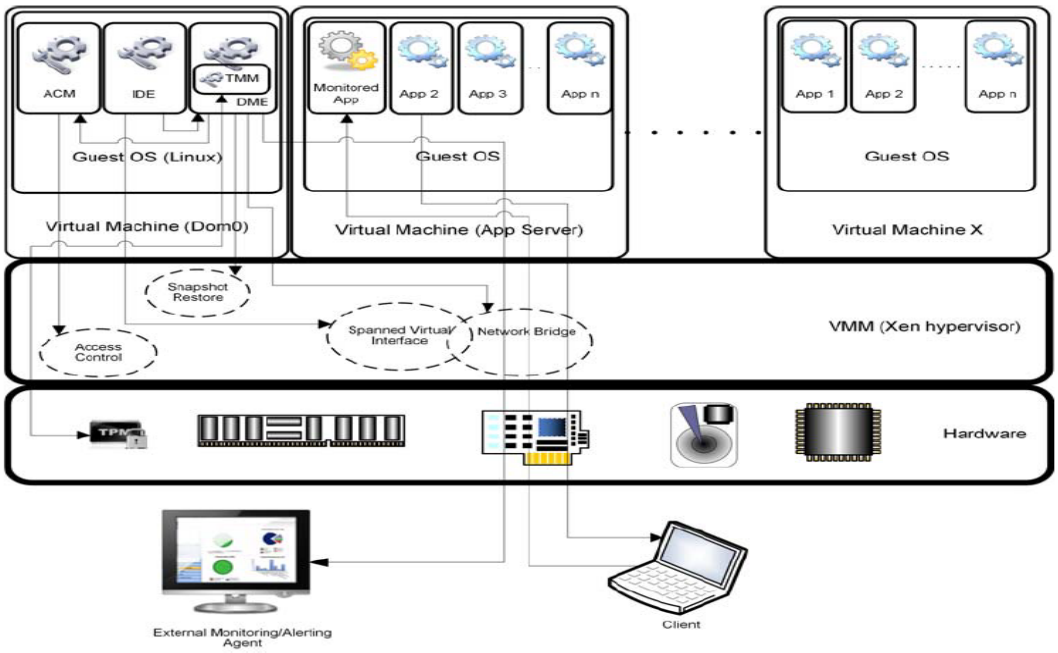

Figure 3: Integrated security services hosted in virtual environments. A diagram from Jayarathna D. et al. [15]

2.4.3 A Cloud Security Framework Based on Trust Model and Mobile Agent

Benabied S. et al. [16] In their paper proposed a two levels security framework based on continuous examination of trust degree, a trust model is used to calculate the trust degree of each user, and to monitor his behavior and activities. According to them, it is beneficial for updating security policies, to prevent unauthorized accesses to cloud data and for protecting information against malicious users and misuse. It is based also, on mobile agent's technology and their features for cloud computing security. The architecture uses mobile agents as a communication entity which helps to reduce traffic on the network, to reduce workload at cloud service provider, to reduce the amount of information exchanged between user and CSP, so, it minimizes the chance to intercept the exchanged information across the network, also, the user can monitor the privacy of his data without relying on CSP information. They propose the following: the use of multiple mobile agents for accounting and monitoring the virtual machines at CSP, in order to improve the quality of the proposed solution and to give the user more visibility in his own information and to reinforce the trust between users and Cloud provider.

2.4.4 Security in Container-based Virtualization through vTPM

Hosseinzadeh S., et al.,2016, [17] in their paper, Figure 1.7 below, they have placed the software TPMs inside just another container.

This special vTPM management container can have access to the hardware-based TPM and expose vTPM interface to the other containers through a communication channel.

In practice, this channel can be local UNIX domain socket or another IPC mechanism.

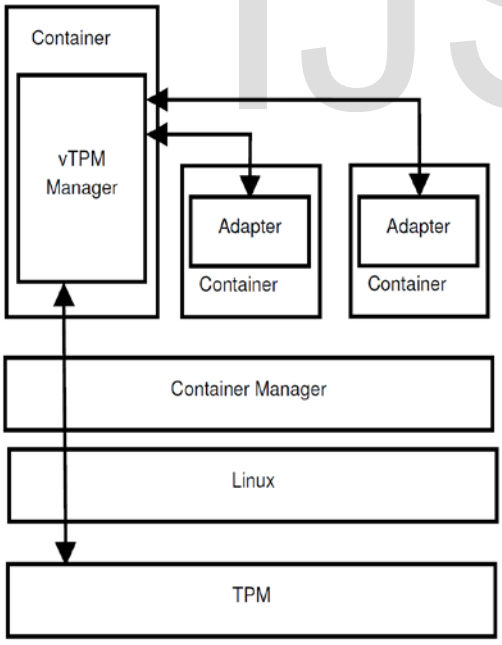

Figure 4:security in container-based virtualization through VTPM as proposed by Hosseinzadeh S., et al.,2016, [17] in their paper.

2.4.5 Using Trusted Platform Module (TPM) to Secure Business Communication (SBC) in VANET

Sumera I., et al. [18] presented the secure business communication (SBC) architecture. They use TPM inside the smart vehicle for security. TPM is a fundamental component of SBC architecturethat ensures there is secure communication between a user and business parties in VANET (Vehicular Ad-hoc Network).

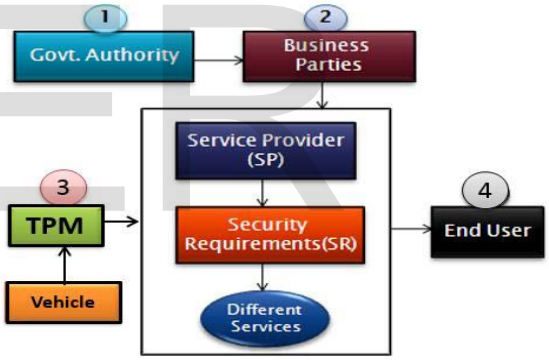

Figure 5: Proposed SBC Model by Sumera I., et al. [18].

VANET potential applications directly focus on the safety of its users on the road by sending some safety messages and non-safety messages. Sumera adds that for successful implementation of business model every module plays their role accurately and serves the end users. Security and privacy are most important factors for real implementation of the business model.

2.4.6 Enhancing Cloud Security and Privacy:The Unikernel Solution

Bratterud A et al. [19] introduced a framework for classifying unikernel systems, with the aim of designing a framework to provide a secure approach to the challenges of cloud security and privacy.

Their solution was to find and solve the challenges

brought about by the audit trail issues. This will require a secure internal communication, log storage and a strong forensic trail. Once these security solutions are in place, then attention is focused on privacy.

2.4.7 Implementation of User Authentication as a Service for Cloud Network

Shah M et al. [13] in their paper is based on the proposed model to provide central authentication technique so that secured access of resources can be provided to users instead of adopting some unordered user authentication techniques.

They propose a model for providing authentication

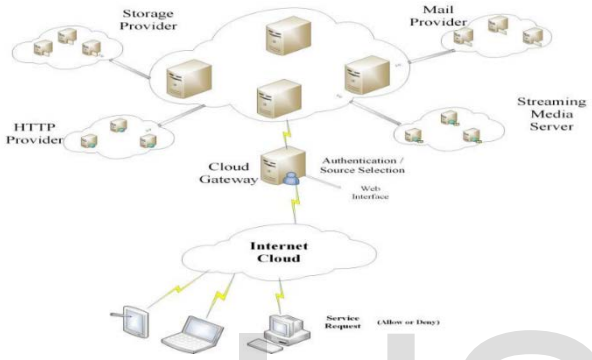

Figure 6: User Authentication as a Service for Cloud Network as proposed by Shah M et al. [13] in their paper**.**

2.4.8 Design and Implementation of Security in Healthcare Cloud Computing

According to Gorata M [20], cloud computing has not only benefited the information technology community, even the healthcare organizations are benefiting from this technology. The sharing of health information on the cloud had made it easy for health professionals to access patient's information from anywhere around the world. Treatment of patients has now been made easy because the patient history is now available on the cloud. Although the whole world is greatly benefiting from this technology, there are also some issues with the security of data in the cloud. Strong security measures should be implemented so that data does not fall into the wrong hands. A mathematical model is proposed in this study for computing availability of information and servers on cloud computing. This model considers both data and node availability parameters which some of them are static during the cloud lifetime and others have dynamic nature. That means they can change based on the resource capacity or can be varying based on the different algorithm that the systems use. The paper also presents the current state-of-the-art research in this field by focusing on several shortcomings ofcurrent healthcare solutions and standards and they further proposed a system that will encrypt data before it is being sent to the cloud. The system is intended to be linked to the cloud in such a way that, before the client submits the data to the cloud the data will go through that system for encryption. The paper presents the steps to achieve the proposed system and a sample of the encrypted and decrypted file using our proposed method is given.

to the users of cloud computing has been presented. Window Server 2008, ESXi Server and Windows 7 were installed to create the cloud environment. Data protection to the resources was provided through a web-based authentication server. The user authentication is the additional overhead for the companies besides the management of availability of cloud services. In the paper, they tried to reduce the overhead of the companies using cloud computing. The model just implemented as a prototype, they recommend to increase more security using signatures and add more services into the circle of authentication.

2.4.9 Multi-level Intrusion detection system in cloud environment based on trust level

Salek Z. et al. [21] proposed a cloud computing architecture based on different trust levels. They introduced users labels such as "Not Trusted", "trusted" or "Highly trusted" to represent the risk level of users. When the risk level of VM user is identified the dispatching agent chooses the accommodation type of IDS and send a chosen IDS agent to the users VM.

They evaluated their model using Snort and by optimally adjusting it for each cloud service security level. Their results show that it's possible to reduce processing time and drop packet rate, with a slight decrease in accuracy, on average therefore enabling the cloud provider to handle more traffic loads with the same resources.

2.5 Cloud security requirements

The requirements that any secure cloud server should satisfy during VM migration are:***1) Confidentiality:***confidential data is considered to be sensitive. Cloud computing objective is usually to allow only authorized users to view the data and also

protection of data from accidental or intentional unauthorized access by internal or external parties.***2) Authorization:*** there is an increase of the risk of unauthorized access to data due to sharing of a common infrastructure in the cloud computing.***3) Integrity:*** This is whereby data from one customer may be contaminated with those from another customer or accessed by another customer.

4) Trust chain/mechanism:The chain of trust has to be well established in that only trusted servers can receive correct VMs and/or vTPMs

5)Authenticity:Only authorized entities should be allowed to initiate migration process. This prevents attacks on the whole system.

3 DISCUSSION

From literature, there exists a number of cloud computing security architectures which can be used in different cloud layers' platforms. Most of the literature is focused on user Authentication, software Authenticity and Trust chain mechanism. A little of the existing work has been done in relation to cloud migration security.

From table 1 several architectures have been proposed using different methods for various application in the cloud. We compared each of the existing architectures in terms of the security requirements of the cloud migration and found some of the strengths and weaknesses of each.

Yu Z., et al. [14], Jayarathna D. et al. [15] and Hosseinzadeh S., et al. [17] proposed models that uses vTPM. Additionally, Yu Z., et al. combined a trust system that applies CA and TPM in their architecture. Their model meets all the security requirements studied in this paper. On the other hand, Jayarathna D. et al.introduced an architecture that combines TPM with hypervisor level access control and IDS [15]. Hosseinzadeh S., et al. placedthe software TPMs inside just another container. The vTPM management container can have access to the hardware-based TPM and expose vTPM interface to the other containers through a communication channel.

Bratterud A et al. presented a framework for classifying unikernel systems. Their focus was on reducing the software attacks for a cloud-based system [19].

Shah M et al. [13] proposed a central authentication technique so that secured access of resources can be provided to users. Additionally, the y developed a prototype of the proposed technique. They recommended use of signatures and addition of more services into authentication.

Benabied S. et al. proposed a two levels trust model based on examination of trust degree, it calculates the trust degree of each user, and monitor user behavior and activities. Their model is based on mobile agent's technology [16].

Gorata M [20] proposed a mathematical model for computing availability of information and servers on cloud computing for healthcare.

In their paper, Salek Z. et al. [21] proposed a multi-level IDS for cloud computing using trust levels. Theyuse these labels in their work to determine the risk level for each user and finally, they evaluated their model using Snort.

From the published literature there exist some loopholes as summarized below:

i ***Insufficient Access Control***

In our analysis, we found out that some proposed solutions lacked the sufficient access control in terms of authorization to the VMs and between the VMs

ii ***Lack of Mutual Authentication***

Once migration VMs are in transit, they need to be authenticated from both the migrating VM and the receiver VM. This is lacking in some of the solutions proposed**.**

iii ***Lack of Confidentiality***

Only authorized parties of the system have the ability to access protected data. The more the number of parties increases the high risks of unauthorized parties accessing the data. From literature, confidentiality security measure is still lacking.

iv ***Lack of Integrity***

Integrity is protecting data from an unauthorized deletion, modification and fabrication. In some of the solutions analyzed, this is not sufficiently taken care of.

From table 1, we can deduce that the models that have insufficient access control in terms of authorization to VMs and between VMs are four, those that lack mutual authentication are three, those that lack confidentiality are two and those that lack integrity are two from the eight models of virtual machine migration that have been analyzed.

Additionally, there are other security requirements that were analyzed in this paper and includes the different methods every model used, their trust chain mechanism and whether they fully cater for the issue of VMs migration. Our table 1 shows only one model that fully embraced VMs migration while three other models do not incorporate the trust chain mechanism.

TABLE 1 STRENGTHS AND WEAKNESSES OF THE EXISTING ARCHITECTURES

Security Requirements	1	2	3	4	5	6	7	8
	A TPM and CA Architecture [14]	Integrated Security for Services Hosted in Virtual Environments [15]	A Cloud Security Framework Based on Trust Model and Mobile Agent [16]	Security in Container-based Virtualization through vTPM [17]	Enhancing Cloud Security and Privacy: The Unikernel Solution [19]	Implementation of User Authentication as a Service for Cloud Network [13]	Design and Implementation of Security in Healthcare Cloud Computing [20]	Multi-level Intrusion detection system in cloud environment based on trust level [21]
Confidentiality	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Authorization	Yes	No	Yes	Yes	No	Yes	No	No
Integrity	Yes	Yes	Yes	No	No	No	Yes	No
Trust chain/mechanism	Yes	Yes	Yes	Yes	No	No	No	Yes
Authentication	Yes	No	Yes	Yes	Yes	No	Yes	No
Migration	Yes	No	No	No	No	No	No	No
Method	CA/TPM	TPM	Agent-Based Trust Model	Container-Based vTPM	Unikernel Solution	User Authentication	Mathematical Model	Multilevel IDS

4 CONCLUSION AND FUTURE WORK

The threat of data compromise increases in the cloud due to an increased number of parties, devices and applications involved. In the case of data integrity, assets can be modified by only authorized users in authorized ways. In this work, we have critically analyzed the published literature on the security of the cloud and different architectures and the methods used.

From literature, a TPM and CA Architecture proposed by Yu Z., et al. [14], is perceived as a better model to overcome some of the challenges of cloud computing during migration as well as take care of the security requirements in the cloud.

However, a different approach needs to be tried using a different migration key for authentication, encryption of the VMs and updating the key manager.

AUTHORSHIP

- *Sam Njuki is currently pursuing PhD program in computer science and Technology in Beijing University of Technology,, China,. E-mail: samnjuki@emails.bjut.edu.cn.*
- *Jianbiao Zhangis a Professor in college of computer science and Technology , Beijing University of Technology,, China,. E-mail: zjb@bjut.edu.cn.*
- *Edna Too is currently pursuing PhD program in computer science and Technology in Beijing University of Technology,, China,. E-mail: tooedna@emails.bjut.edu.cn.*

5 REFERENCES

[1] S. Venkata, K. Kumar, and S. Padmapriya, "A Survey on Cloud Computing Security Threats and Vulnerabilities," Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng., vol. 2, no. 1, pp. 622–625, 2014.

[2] C. C. Rao and A.V.Ramana, "Data Security in Cloud Computing," Int. J. Curr. Trends Eng. Res., vol. 2, no. 4, pp. 84–92, 2016.

[3] C. Chen, H. Raj, S. Saroiu, I. Nsdi, and A. Wolman, "cTPM : A Cloud TPM for Cross-Device Trusted Applications," 11th USENIX Conf. Networked Syst. Des. Implement., vol. 8, pp. 187–201, 2014.

[4] R. Konnur, K. Dullolli, and S. Kundgol, "Security Threats in Cloud Computing," Int. J. Innov. Res. Sci. Eng. Technol. (An ISO Certif. Organ., vol. 3297, no. 10, 2016.

[5] A. M. Alzadjali, A. H. Al-Badi, and S. Ali, "An analysis of the security threats and vulnerabilities of cloud computing in Oman," in Proceedings - 2015 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2015, 2015, pp. 423–428.

[6] D. Perez-Botero, J. Szefer, and R. B. Lee, "Characterizing hypervisor vulnerabilities in cloud computing servers," Proc. 2013 Int. Work. Secur. cloud Comput. - Cloud Comput. '13, no. May, p. 3, 2013.

[7] F. Zhang, J. Chen, H. Chen, and B. Zang. Cloudvisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In Proceedings of SOSP, 2011.

[8] M. Shah and A. S. Shah, "Appraisal of the Most Prominent Attacks due to Vulnerabilities in Cloud Computing," Int. J. Grid Distrib. Comput., vol. 9, no. 7, pp. 13–22, 2016.

[9] Himanshu Raj, David Robinson, Talha Bin Tariq, Paul England, Stefan Saroiu, and Alec Wolman. Credo: Trusted Computing for Guest VMs with a Commodity Hypervisor. Technical Report MSR-TR-2011-130, Microsoft Research, 2011.

[10] S. Bulusu and K. Sudia, "A Study on Cloud Computing Security Challenges," Sea-Mist.Se, p. 128, 2012.

[11] M. ArunFera and M. SaravanaPriya, "A survey on trusted platform module for data remanence in cloud," in Advances in Intelligent Systems and Computing, vol. 398, 2016, pp. 689–695.

[12] Bhopale S. D., Cloud migration benefits and its challenges issue,

[13] M. Shah, A. S. Shah, and I. Ijaz, "Implementation of User Authentication as a Service for Cloud Network," Int. J. Grid Distrib. Comput., vol. 9, no. 10, pp. 197–210, 2016.

[14] Z. Yu, W. Zhang, and H. Dai, "A Trusted Architecture for Virtual Machines on Cloud Servers with Trusted Platform Module and Certificate Authority," J. Signal Process. Syst., vol. 86, no. 2–3, pp. 327–336, 2017.

[15] D. Jayarathna, V. Varadharajan, and U. Tupakula, "Integrated security for services hosted in virtual environments," Proc. - 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 10th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Symp. Parallel Distrib. Proce, pp. 82–89, 2017.

[16] S. Benabied, A. Zitouni, and M. Djoudi, "A cloud security framework based on trust model and mobile agent," Cloud Technol. Appl. (CloudTech), 2015 Int. Conf., no. January, pp. 1–8, 2015.

[17] Hosseinzadeh S., et al, Security in Container-based Virtualization through vTPM ,2016

[18] I. Sumera and H. Bin Hasbullah, "Using Trusted Platform Module (TPM) to Secure Business Communication (SBC) in Vehicular Ad hoc Network (VANET)," ResearchGate, no. November, pp. 28–33, 2015.

[19] A. Bratterud, A. Happe, and B. Duncan, "Enhancing Cloud Security and Privacy: The Unikernel Solution," Cloud Comput. 2017 Eighth Int. Conf. Cloud Comput. GRIDs, Virtualization, no. February, pp. 1–8, 2017.

[20] M. Gorata, A. M. Zungeru, M. Mangwala, and J. Chuma, "Design and Implementation of Security in Healthcare Cloud Computing," J. Comput. Sci., vol. 13, no. 2, pp. 34–47, 2017.

[21] Z. Salek and F. M. Madani, "Multi-level Intrusion detection system in cloud environment based on trust level," 2016 6th Int. Conf. Comput. Knowl. Eng. ICCKE 2016, no. Iccke, pp. 94–99, 2016.

[22] Trusted Computing Group. TPM Main Specification Level 2 Version 1.2, Revision 130, 2006.