Understanding Cloud Computing Security Problems

Emmy Mugisha*[1], Zhang Gongxuan[2], Lynda BOUKELA[3]

[1]Faculty of Computing and Information Sciences, University of Lay Adventists of Kigali
Kigali, 6392 - Rwanda

[2] School of Computer Science and Engineering, Nanjing University of Science and Technology
Nanjing, 210094 - China
[e-mail: gongxuan@njust.edu.cn]
[3]School of Computer Science and Engineering, Nanjing University of Science and Technology
Nanjing, 210094 – China
[e-mail: boukelalynda@outlook.fr]

*Corresponding author: emymugi@gmail.com

Abstract

Cloud Computing (CC) is elastic, affordable, and tested delivery platform for rendering IT services (i.e. Platform-as-a-Service, Software-as-a-Service and Infrastructure-as-a-Service) to consumers by means of Internet medium. This emerging technology poses certain degree of danger due to the fact that substantial services are frequently outsourced to a third party, hence becoming difficult to preserve data privacy, security, control and availability. In single or multi-cloud, services (PaaS, SaaS, and IaaS) may require migration from one cloud to another, which may become challenging to procure security problems among the two clouds. CC merges a number of different technologies i.e. Web 2.0, virtualization and SOA, which in return acquires their security problems. In this article, we analyze diverse security problems found in CC by discovering the primary vulnerabilities and significant threats encountered from cloud service models (PaaS, SaaS, and IaaS) architectural design and other different areas related to CC and its surround.

Deep learning and literature-based experience on the design and architectural perspectives of the cloud service model method has been employed to discover and analyze the possible security problems that reside on cloud services. The potential result of our work is a detailed possible vulnerabilities and threats that frequently appear to be the main sources of cloud security problems. Based on our results, cloud developer, designer, and providers are now aware of where to put much effort to eliminate and procure security problems for many to adopt cloud services.

Keywords: Threats, Cloud computing, Vulnerabilities, Security, SPI model

INTRODUCTION

Cloud Computing (CC) adoption is rapidly rising attracting apparent lot of attention in the scientific and industrial research. Gartner (2011) studied CC within ten most leading authoritative technologies as the first and promising expectations in sequential ages by cloud players. CC enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

CC shows a distribution architecture with the main objective of providing convenient data storage and network service, secure and quick services in a virtualized environment and accessed via Internet medium (Zhao et al., 2009; Zhang et al., 2010). CC advances scalability, agility, availability, collaboration and ability to adapt variations according to request, access and allows possible cost-effective using optimized and effective tools (Cloud Security Alliance, 2011; Marinos & Briscoe, 2009; Centre for the Protection of National Infrastructure, 2010; Khalid, 2010). Moreover, CC merges a number of computing technologies; that is to say: Web 2.0, Service Oriented Architecture (SOA), virtualization and several technologies are based on Internet to provide common Internet-based services (applications) online using web browsers to meet tenants needs, as their applications/services and data are stored on the servers/datacenters (Marinos & Briscoe, 2009). Furthermore, CC act as the ageing of these technologies and is a commercial term to constitute that ageing and the services they offer (Centre for the Protection of National Infrastructure, 2010). However, though a number of interests to adopting CC; there exist a number of apparent obstacles to its adoption. That is, security, standardization, privacy and legal trends are the major obstacles for CC adoption (KPMG, 2010).

In addition, CC constitutes a comparative novel computing model. However, there remains doubt regarding how security can be attained to all models, as well as how application' security is moved to the cloud (Rosado et al., 2012). This doubt has systematically guided information administrators to express that security is their priority on CC trends (Mather et al., 2009). Security priorities refer to dangerous domains for instance; multi-tenancy, external data storage, public internet dependence. In relation to traditional computing technologies, the cloud consists of several particular characteristics, i.e. large scale, resource distribution by cloud providers, heterogeneity and virtualized. Therefore, security controls for other IT environment doesn't differ from that of CC. However, since cloud service models are utilized, CC might demonstrate unique dangers to an organization with operational models, together with technologies used to enable cloud services than traditional IT solutions.

This paper aim at outlining prior security problems in CC; this will account vulnerabilities, threats, as well as results as an answer for security in CC environment. Therefore, the research question addressed is: What are security vulnerabilities and threats in CC environment which have to be considered, studied and handled?

Here, we demonstrate CC security problems targeting SPI model by pointing security problems found in CC and discovering the primary vulnerabilities and significant threats encountered from different areas related to CC. A threat is a possible attack leading to information or resources abuse. Looking into the literature of CC, many studies have been conducted on one service model or only by listing cloud security problems in a wide view without distinguishing among vulnerabilities and threats. Here, we demonstrate a number of possible vulnerabilities and threats, and also point out how cloud service models can be affected. Furthermore, we also demonstrate some security analysis related to these threats which try to solve or improve the identified problems.

The remainder of the paper is organized as follows: Section 2 describes our research and discussions. In Section 3, we specify the most significant security views of the Cloud models. Section 4 presents analyses of security problems in CC by pointing out the main vulnerabilities and the most significant threats in clouds. Finally, in section 5 we provide some conclusions.

RESEARCH AND DISCUSSIONS

The research discussed in this paper identifies, classifies, analyzes, and lists a number of vulnerabilities and threats as illustrated in Section 3 with regard to CC. The paper analyzes the threats and risks, along with recommendations to overcome them. Moreover, adding to our literature review, threats and vulnerabilities demonstration, we also tackled problems associated with security in the cloud environment.

The SPI models

CC model offers three types of services

(Subashini & Kavitha, 2011; Mell, & Grance, 201; Zhang et al., 2010):

Software-as-a-service (SaaS) - This is the capability provisioned to the consumer to use applications running on cloud provider's infrastructure. These applications can be retrieved or accessed by a number of devices through a web browser interface e.g., web-based email.

Platform-as-a-Service (PaaS) - This is a service capable of offering a cloud infrastructure to the consumer to outsource his or her own applications in absence of installing tools, i.e. operating system support and software development frameworks on his or her local units.

Infrastructure-as-a-Service (IaaS): This service gives the consumer ability to utilize CPU, storage, networks, as well as other basic computing capabilities.

Therefore, for SaaS, the security load occurs on the cloud provider's side due to the degree of abstraction. SaaS service model is built on a peak functions integrated under less customer hands or monitoring. Unlikely, the PaaS model provides mechanism for customer monitoring and control over their resources. Therefore, as the matter of facts, IaaS is proved to have lower degree of abstraction and implements reliable customer control over security than PaaS or SaaS (Mather et al., 2009).

Understanding security disputes in the field of CC, similarities and dependability between cloud service models has to be elaborated first (Cloud Security Alliance, 2011). SaaS as well as PaaS are built on top of IaaS whereby an attacker on IaaS, it is very apparent that it must influence others i.e. SaaS and PaaS services. Hence, per cloud service model, they hold unique dependable security holes; therefore, they also have in common several implications that impact them as well. In addition to that, each model is capable of securing its own services in terms of security, this arises the problem of lack of standardization among providers in terms of enhancing security which have to result incompatibility during abstraction of security models.

Software as a Service Security Problem

SaaS offers application services on-demand basis, for instance conferencing software, email and business applications, i.e. Supply Chain Management (SCM), Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) (Ju et al., 2010). SaaS consumers have limited security control within the three fundamental delivery models in the cloud. Therefore, the implementation of SaaS services may raise some security indicators.

Application security: For applications, this service is generally delivered through Internet using a web browser (Rittinghouse & Ransome, 2009; Jensen et al., 2009). Hence, security holes in web applications produce vulnerabilities for the SaaS applications attack. Attackers use web to enter tenant's computing resources and execute harmful or dangerous actions, for example theft of important data (Zhang et al., 2010). Furthermore, security concerns in SaaS applications do not differ much from other web application technologies. Nevertheless, security solutions for the past decades cannot handle today's hacker's behavior effectively. Consequently, new solutions need to be found (Mell & Grance, 2011). In that sense, ten dominating crucial web application security breaches were outlined by Open Web Application Security Project (OWASP). Table 1 depicts the study results studied web-based vulnerabilities in past consecutive years (Wei et al., 2009).

Table. 1 Vulnerability study results

Year	Number of
2012	4, 310
2013	3, 499
2014	4, 340
2015	4, 699
2016	7, 020

Multi-tenancy: SaaS applications seemingly as maturity models that are characterized by multi-tenancy, scalability and configurability via metadata (Rittinghouse & Ransome, 2009; Owens, 2010). At first, each customer is assigned his own customized instance of the application, and that is maturity model. The model returns some weakness as security problems are less concerned compared with the other models. In the following model, the provider offers unique application instances to a certain customer or service subscribers; however the total application instances inherit the same application code. Furthermore, customers may alter limited alternative configurations to certify their goals. In addition, multi-tenancy model is followed whereby a standalone instance serves other customers (Chong et al., 2006). This model allows efficient resources utilization with scalability issues. That is, data accessed from different multiple tenants is potentially collocated in the same datacenter, this poses data leakage problem. Henceforth, customer data requires strong security policies to enforce independent data storage among customers (Bezemer & Zaidman, 2010). Application migration as the final model, here applications need to be scaled up or migrated to a secure or capable server whenever required by customers. Fig. 1 shows the increase in vulnerable cases in web-based application securities.

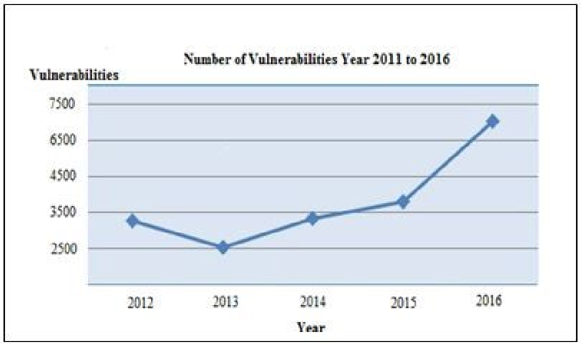

Fig.1. Estimated detected vulnerabilities between 2011 and 2016

Data security: Data security is a serious aspect posed wherever computing technologies is applied. However, it results in a serious question whereby SaaS tenants or subscribers rely on their providers for trusted and robust security (Jensen et al., 2009; Mell & Grance, 2011; Viega, 2009). Deeper in SaaS, data management is mostly managed in cleartext or plaintext and then deposited in the cloud storage datacenters. For SaaS, the software provider holds customer data management and security as well as storage is concerned (Wei et al., 2009). Furthermore, data failure and loss requires backup or recovery. This is seemingly critical in case of disaster, hence posing security concerns during recovery procedures (Mell & Grance, 2011). Consequently, cloud providers may lend some extra services from other providers, i.e. backup from third-party service providers. This may pose a lot to customer side in terms of secure service accessibility. In addition, current applicable interoperability standards do not figure out its application in the field of CC (Jensen, 2009). With SaaS, the act of standardization is critical due to the fact that data is accessed from provider's side, which poses restriction issues, i.e. data security, privacy and segregation and this has to be implemented by the provider.

Accessibility: The process of accessing applications through the internet medium using web browsers returns pooled devices on different network easier; that is to say, publicly utilized computers and mobile devices. In the same sense, this remote accessibility opens vulnerable holes against the service hence security risks. It has been released out that the current top mobile computing threats are; insecure networks (wireless), mobile malware, information theft and vulnerabilities. All these were reported from device operating system (OS) and official applications, insecure marketplaces, and proximity-based hacking (Cloud Security Alliance, 2012).

Platform-as-a-Service (PaaS) Security Problems

For PaaS, it helps cloud-based applications deployment with no highly skilled customers on setup, cost of configuring or buying and preserving the hardware and software layers evolved (Mell & Grance, 2011). However, knowing well that PaaS inherits security from a secure web browser and reliable network, the security of PaaS application shows two layers: 1) the security of the PaaS and 2) the security of customer applications deployed on the PaaS (Mather et al., 2009). Therefore, securing the platform core areas, i.e. the runtime engine that runs the customer applications is implemented by the platform providers.

Infrastructure-as-a-Aervice (IaaS) Security Problems

IaaS offers pool of resources, i.e. network devices, storage, server etc, in a virtualized form via Internet medium (Wang et al., 2009). With this, consumers can execute possible software or application or a virtualized resource with entire management on the resources assigned to them (Dahbur et al., 2011). In addition to that, comparing to other service models, IaaS demonstrate efficient security management tenants, given that no security hole in the virtual machine monitor (Mell & Grance, 2011). Moreover, tenants are provided means to control software running on their virtual machines, and capable of security policy configurations effectively (Jaeger & Schiffman, 2010). Still, pooled resources, for instance; storage network and other computing units, all in one as cloud infrastructures are supervised and managed by cloud providers. Finally, an IaaS provider holds a big part to enforce secure cloud infrastructure as a good start to handle and reduce these threats.

In Virtual networks, as a nature of resource pooling, network devices are shared by many different tenants. This pool of resources opens or gives attackers a hole to launch cross-tenant attacks as mentioned earlier (Grobauer et al., 2011). Therefore, virtual network components increase networked VMs; this alerts a special security risk in CC (Wu et al., 2010). However, to improve VM security is to separate each VM via possible physical channels. Furthermore, different hypervisors use virtual networks to connect virtual machines physically and efficiently.

They are two reported ways of providing link between virtual networks, i.e. bridged and routed. However, these ways increase the risk to sniffing and spoofing virtual network successfully (Subashini & Kavitha, 2011; Xiaopeng et al., 2010).

CLOUD SECURITY PROBLEMS

Here, the analysis of current surviving security vulnerabilities and threats in CC is described. Expanding, each vulnerability and threat impacts cloud service model or models. Table 2 demonstrates an analysis of vulnerabilities in CC. The analysis contributes a basic interpretation of vulnerabilities, and point out particular cloud service models (SPI) expected to be impacted.

We look at technology-oriented vulnerabilities, where some institutional common vulnerability needs much attention since they harm the security policy of the cloud. Unprofessional strategy of employee recruitment and briefing with regard to security policy (Cloud Security Alliance, 2010); authorized tenants, i.e. cloud executives holds full access to the cloud data. Lacking occasional customer desktop controls which may lead to unauthorized or adversary to open an account with a valid credit card and email. Apocryphal accounts can allow unauthorized or adversary to perform malicious action unknowingly (Cloud Security Alliance, 2010). Lack of security education or guidelines can allow tenants as weak point to pose information security vulnerability (Popovic & Hocenski, 2010).

CC merges a number of new and old technologies such as virtualization, web browsers and web services that leads to the development of cloud concept. In addition to that, given that these technologies are vulnerable to the attacker, it will as well be vulnerable to the cloud, hence compromised. Considering Table 2, it is very clear that virtualization and data storage are prior critical aspect. Moreover, compromising lower layers implies other layers as well. Table 3 summarizes different threats in CC. It also depicts the threats that are inherited from vulnerable technologies merged in cloud environments, and we continue by showing cloud service models that are likely to be compromised by these threats. We look at threats linked to virtualization, resource pool and remote data storage and accessibility.

Table 2. Vulnerabilities in cloud computing

Vulnerabilities	Service	Description
Data-associated vulnerabilities	SPI	Data may be located or stored in several different jurisdiction with different SLA (Ertaul et al., 2010; Carlin & Curran, 2011; Bisong & Rahman, 2011); From there, data can be accommodated together with hackers, with no strong separation mechanism (Viega, 2009), again, tenants are not aware of where their data is located (Jansen, 2011). Given that a tenant decides to leave the cloud, s/he cannot trust if his data was completely deleted from the cloud (Ertaul et al., 2010; Grobauer et al., 2011; Jansen, 2011; Townsend, 2009). Data storage, access, and transmission occur in form of plaintext which makes it easy to hackers to access useful information.
Unlimited allocation of resources	SPI	Wrong resource utilization modeling may contribute to over-provisioning (ENISA, 2009).
Vulnerabilities in virtual networks	I	Virtual bridges shared by various VMs (Wu et al., 2010).

Unsafe APIs & UI	SPI	Cloud providers extend services via APIs (SOAP or REST & HTTP) (Dawoud et al., 2010). The cloud is required to secure its interface so as its service accessibility to be safe (Cloud Security Alliance, 2010). Cloud APIs are still in early evolution as it upgrades timely and that can become a door for an attack (Carlin & Curran, 2011).
Vulnerabilities in VMs	I	Virtual Machines have IP addresses visible to all logged into the cloud, this allows hackers to map VM location (Ristenpart et al., 2009); lack of VMs migration control from server to server may result a serious danger (Dawoud et al., 2010; Garfinkel & Rosenblum, M. Rosenblum, 2005).

The purpose of this research is also to identify current defenses that can defeat apparent threats. This information can be extracted deeper by using misuse patterns (Fernandez et al., 2009). To this far, misuse patterns account how a misuse is executed by the hacker. For example, a hacker can read or change the contents of the VM state files while on live migration due to the insecure network lines; i.e. Internet. To tackle this insecure VM migration, different techniques: TCCP (Santos et al., 2009) that allows crucial execution of VMs and secure migration processes is proposed. In a condition where a VMM-protected system is demonstrated and active, a secure migration tool capable of VM live migration was introduced in PALM (Zhang, 2008). In addition, malicious VM creation is a dangerous cloud threat whereby an adversary manipulates malicious VM image holding malware. Malicious VM manipulation is practicable as long as any valid cloud tenant can create a VM image and submit it to the cloud's servers to which multiple tenants can access them. Given that the malicious VM image manipulated or created holds malware or harmful bugs, it will inject collocated VMs. Therefore, to overcome this threat, the security management characteristics, i.e. access control framework, image filters, provenance tracking system, and repository maintenance services was suggested by Mirage (Wei et al., 2009). Table (3) show some detailed common threats in the clouds.

Table. 3 Threats in cloud computing

Threat	Service	Description
Data leakages	SPI	Data leakages take place during the time tenant's data or information is redirected to a harm address as is in transit, stored, audited or processed (Cloud Security Alliance, 2010; Wu et at., 2010; Grobauer, 2011; Ristenpart et al., 2009).
Data scavenging	SPI	Deleted tenant data can still be restored by hackers, since data cannot be permanently deleted until the device or resource is destroyed (Mather et al., 2009; ENISA, 2009; Jansen, 2011).
Service Hijacking	SPI	A service hijack can be done in different ways, i.e. social engineering. If an adversary wins access to a service tenant's important information, s/he is likely to act malicious actions such as access to secret data, changes data, and reverse services (Cloud Security Alliance, 2010).
Denial of service	SPI	Malicious tenants are anticipated to gain access to all resources. Hence, the cloud will suffer resource availability in case other tenants requests.
VM escape	I	This targets hypervisor with the goal of gaining management of the fundamental infrastructure in the cloud (Morsy et al., 2010; Wang et al., 2009).

Customer-data manipulation	S	Tenant's web application abuse by faking data sent from their application part to the cloud servers (Grobauer et al., 2011; OWASP, 2010).
Malicious VM creation	I	A legitimate account might become an adversary by creating a valid VM image with malicious scripts such as a Trojan horse and disperse them in the cloud storage (Grobauer et al., 2011).
VM hopping	I	It occurs when a VM is able to gain access to another VM via open vulnerability (ENISA, 2009; Jasti et al., 2010).
Sniffing virtual network	I	A virtual network packet can be reversed to other VMs by use of ARP spoofing as a result of a harmful VM hopping (Reuben, 2007; Wu et al., 2010).
Insecure VM migration	I	Live VMs migration discloses log file contents to the network which allows hackers to access, redirect the VM to unexpected address (Dawoud et al., 2010;

CLOUD SECURITY ANALYSIS

In this section, we provide a detailed review on some specific individual security measures with respect to SPI models.

Service Hijacking

Active Credentials: An algorithm to produce or return active credentials for mobile cloud computing systems is presented (Xiao & Gong, 2010). Given that a tenant changes his or her geographical location or alters network, his or her active credential value corresponds with his or her current address or network.

Access and identity management guidance: A non-profit body that advances utilization of best findings to support, offer and recommend secure cloud environments is termed as Cloud Security Alliance (CSA), CSA published Access and Identity Management Guidance that list recommended best findings to guarantee identities and secure access management (Cloud Security Alliance, 2012). Consequently, the list displays identity management, tenant access certifications, access management, identity and access reporting, privileged tenant and separation of duties, role-based access control, and centralized directory.

Customer Data Manipulation

Web Application Scanners: For web browsers, applications become target due to its nature of publicly exposed to potential attackers. Therefore, web application scanners (Fong & Okun, 2007) act as a tool that scans web applications services to discover security vulnerabilities evolved in the application for immediate fix. Fig. 2 shows scanned vulnerabilities in a specific time.

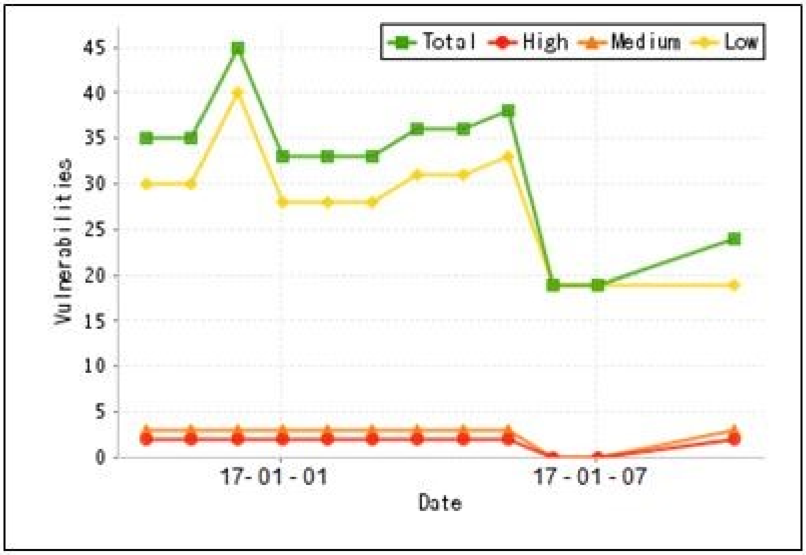

Fig. 2 Vulnerability degree in a specific period

Virtual Machine Escape

Hyper-Safe: Hyper-Safe offers hypervisor control-flow integrity. The idea is based on two aspects; i.e. 1) non-by-passable memory lockdown which protects write-protected memory pages and 2) restricted pointed indexing that converts control data into pointer indexes (Wang & Jiang, 2010) both targeting to guard type I hypervisors. Moreover, to assess the strength of this finding, four types of attacks were carried on; i.e. hypervisor code manipulation, running injected code, changing the page table, and tamper from a return table they assessed. Therefore, their Hyper-Safe perfectly blocked all mentioned attacks and also the performance overhead is low.

Trusted Cloud Computing Platform (TCCP): TCCP allows cloud providers to serve closed box execution platforms, and permits tenants to judge if the platform is trusted before launching their VMs (Zhang et al., 2008). It also appends two basic aspects: Trusted Virtual Machines Monitor (TVMM) and a Trusted Coordinator (TC). In addition, TC controls a group of trusted units that run TVMMs, and it is controlled by a trusted third party. In addition, TC plays part in the process of VM migration, which monitors if VM is running on a trusted platform. However, discussions in (Han-zhang & Liu-sheng, 2010) TCCP show an apparent disadvantage whereby all the services have to certify with the TC which outcomes overload. As a result, Direct Anonymous Attestation (DAA) and Privacy CA scheme was presented.

Trusted Virtual Datacenters (TVDc): In (Berger et al., 2008; Berger, 2009), it guarantees separation and integrity in cloud environments. Also, it combines VMs with identical tasks into a Trusted Virtual Domains (TVDs). TVDc guarantees separation between TVDs by imposing required access control, hypervisor-based separation, and secure medium; i.e. VLANs. It also presents integrity by applying load-time attestation method to certify system integrity.

Sniffing Virtual Networks

Virtual network security: For VN, a virtual network model to secure the communication among VN is presented in (Wu et al., 2010). However, the model is rooted on Xen that allows two VNs configuration modes; i.e. bridged and routed. It is made up of three layers: shared networks, firewall and routing layers that guards VMs from spoofing and sniffing.

Insecure VM migration

Protection aegis *for live migration of VMs (PALM):* For live VMs migration, a secure live migration model that maintains integrity and privacy aegis throughout migration process is proposed (Wei et al., 2009). Moreover, PALM was built based on Xen and GNU Linux. The analysis show that this model reports a low degree downtime and migration time as a result of encryption and decryption processes.

CONCLUSIONS

CC is a new technology that demonstrates attractive benefits for its tenants; however, it also raises some security issues that anticipate delaying its adoption speed. Therefore, having more knowledge and awareness on vulnerabilities evolved in CC will ease customers to migrate to the cloud.

As CC merges a number of distinct technologies, it also acquires their security holes hence compromised as well. In addition, we have reviewed virtualization, data storage and traditional web applications, and our analysis shows that the current research demonstrated are not robust based on the current vulnerabilities and threats. Therefore, we have demonstrated current security problems in the cloud service models. Moreover, networks, virtualization and storage are reported to be the most vulnerable to security problems in CC environment.

In that sense, many researchers in this field have discussed security problems in CC but never tried to figure out the distinction between vulnerabilities and threats. In this paper, we have focused on providing the difference and understanding of these problems. As a result, many research findings were outlined in regards to minimize these vulnerabilities and threats. Nevertheless, upgraded security methods are required together with updated traditional methods to build robust cloud architectures.

ACKNOWLEDGMENTS

This work was partly supported by a grant from National Natural Science Foundation Grant NSF 61272420 through the second author.

REFERENCES

Gartner Inc, (2011), “Gartner identifies the Top 10 strategic technologies for 2011”, http://www.gartner.com/it/page.jsp?id=1454221

Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X. & Tang, N. (2009), “Cloud Computing: A Statistics Aspect of Tenants”, In *First International Conference on Cloud Computing (CloudCom)*, Beijing, China. Springer Berlin, Heidelberg, pp 347–358.

Zhang, S., Zhang, S., Chen, X. & Huo, X. (2010), “Cloud Computing Research and Development Trend”, In *Second International Conference on Future Networks (ICFN’10)*, Sanya, Hainan, China, IEEE Computer Society, Washington, DC, USA, pp 93–97.

Cloud Security Alliance, (2011), “Security guidance for critical areas of focus in Cloud Computing V3.0”, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Marinos, A. & Briscoe, G. (2009), “Community Cloud Computing”, In *1st International Conference on Cloud*

Computing (CloudCom), Beijing, China, Springer-Verlag Berlin, Heidelberg Centre for the Protection of National Infrastructure, (2010), "Information Security Briefing 01/2010 Cloud Computing", http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

Khalid, A. (2010), "Cloud Computing: applying issues in Small Business", *International Conference on Signal Acquisition and Processing (ICSAP'10),* pp 278–281

KPMG, (2010), "From hype to future: KPMG's 2010 Cloud Computing survey", http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs-2010-cloud-computing-survey/2384291

Rosado, D.G., Gómez, R., Mellado, D. & Fernández-Medina, E. (2012), "Security analysis in the migration to cloud environments", *Future Internet*, Vol. 4, pp. 469–487

Mather, T., Kumaraswamy, S. & Latif, S. (2009), "Cloud Security and Privacy", *O'Reilly Media, Inc.*, Sebastopol, CA

Subashini, S. & Kavitha, V. (2011), "A survey on Security issues in service delivery models of Cloud Computing", *Journal of Network Computer Application*, Vol. 34, pp. 1–11.

Mell, P. & Grance, T. (2011), "The NIST definition of Cloud Computing", *NIST, Special Publication 800–145*, Gaithersburg, MD

Zhang, Q., Cheng, L. &Boutaba, R. (2010), "Cloud Computing: state-of-the-art and research challenges", *Journal of Internet Services Applications*, Vol. 1, pp. 7–18.

Ju, J., Wang, Y., Fu, J., Wu, J. & Lin, Z. (2010), "Research on Key Technology in SaaS", In *International Conference on Intelligent Computing and Cognitive Informatics (ICICCI)*, Hangzhou, China, IEEE Computer Society, Washington, DC, USA, pp 384–387.

Rittinghouse, J.W. and Ransome, J.F. (2009), "Security in the Cloud", In *Cloud Computing. Implementation, Management, and Security*, CRC Press

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L.L. (2009), "On technical Security issues in Cloud Computing", In *IEEE International conference on Cloud Computing (CLOUD'09)*, Vol. 116, pp. 109–116.

Zhang, Y., Liu, S. & Meng, X. (2009), "Towards high level SaaS maturity model: methods and case study", In *Services Computing conference*. APSCC, IEEE Asia-Pacific, pp 273–278.

Owens, D. (2010), "Securing elasticity in the Cloud", *Commun ACM*, 53(6):46–51.

Chong, F., Carraro, G. & Wolter, R. (2006), "Multi-tenant data architecture", http://msdn.microsoft.com/en-us/library/aa479086.aspx

Bezemer, C.P. & Zaidman, A. (2010), "Multi-tenant SaaS applications: maintenance dream or nightmare?", In *Proceedings of the Joint ERCIM Workshop on Software Evolution (EVOL) and International Workshop on Principles of Software Evolution (IWPSE)*, Antwerp, Belgium. ACM New York, NY, USA, pp 88–92.

Cloud Security Alliance, (2012), "Security guidance for critical areas of Mobile Computing", https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf,

Dahbur, K., Mohammad, B. & Tarakji, A.B. (2011), "A survey of risks, threats and vulnerabilities in Cloud Computing", In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications,* Amman, Jordan, pp 1–6.

Jaeger, T. & Schiffman, J. (2010), "Outlook: cloudy with a chance of Security challenges and improvements", *IEEE Security Privacy,* Vol. 8, pp. 77–80.

Xiaopeng, G., Sumei, W. & Xianqin, C. (2010), "VNSS: a Network Security sandbox for virtual Computing environment", In *IEEE youth conference on information Computing and telecommunications (YC-ICT).* IEEE Computer Society, Washington DC, USA, pp 395–398.

Cloud Security Alliance, (2010), "Top Threats to Cloud Computing V1.0", https://cloudsecurityalliance.org/research/top-threats

Popovic, K. & Hocenski, Z. (2010), "Cloud Computing Security issues and challenges", In Proceedings of the 33rd International convention MIPRO", *IEEE Computer Society,* Washington DC, USA, pp 344–349

Ertaul, L., Singhal, S. & Gökay, S. (2010), "Security challenges in Cloud Computing", *In Proceedings of the 2010 International conference on Security and Management SAM'10*, CSREA Press, Las Vegas, US, pp 36–42.

Carlin, S. & Curran, K. (2011), "Cloud Computing Security", *International Journal of Ambient Computing and Intelligence*, Vol. 3, pp. 38–46.

Bisong, A. & Rahman, S. (2011), "An overview of the Security concerns in Enterprise Cloud Computing", *International Journal of Network Security & Its Applications (IJNSA),* Vol. 3, pp. 30–45.

Viega, J. (2009), "Cloud Computing and the common Man," *Computer,* Vol. 42, pp 106–108.

Jansen, W.A. (2011), "Cloud Hooks: Security and Privacy Issues in Cloud Computing," In *Proceedings of the 44th Hawaii International Conference on System Sciences*, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC, USA, pp 1–10.

Grobauer, B., Walloschek, T. & Stocker, E. (2011), "Understanding Cloud Computing vulnerabilities", *IEEE Security Privacy* Vol. 9, pp. 50–57.

Townsend, M. (2009), "Managing a security program in a cloud computing environment", In *Information Security Curriculum Development Conference*, Kennesaw, Georgia. ACM New York, NY, USA, pp 128–133.

ENISA, (2009), "Cloud Computing: benefits, risks and recommendations for information Security",
ttp://www.enisa.europa.eu/ctivities/riskmanagement/files/deliverables/cloud-computing- risk-assessment

Wu, H., Ding, Y., Winer, C. & Yao, L. (2010), "Network Security for virtual machine in Cloud Computing", In *5th International conference on computer sciences and convergence information technology (ICCIT),* IEEE Computer Society Washington, DC, USA, pp 18–21.

Dawoud, W., Takouna, I. & Meinel, C. (2010), "Infrastructure as a service security: Challenges and solutions", In *the 7th International Conference on Informatics and Systems (INFOS)*, Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, pp 1–8.

Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. (2009), "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", In *Proceedings of the 16th ACM conference on Computer and communications security*, Chicago, Illinois, USA. ACM New York, NY, USA, pp 199–212.

Garfinkel, T. & Rosenblum, M. (2005), "When virtual is harder than real: Security challenges in virtual machine based computing environments", In *Proceedings of the 10th conference on Hot Topics in Operating Systems*, Santa Fe, NM. Volume 10, USENIX Association Berkeley, CA, USA, pp 227–229.

Fernandez, E.B., Yoshioka, N. & Washizaki, H. (2009), "Modeling Misuse Patterns", In Proceedings of the 4th Int. *Workshop on Dependability Aspects of Data Warehousing and Mining Applications (DAWAM 2009)*, *in conjunction with the 4th Int.Conf. on Availability, Reliability, and Security (ARES 2009)*, Fukuoka, Japan. IEEE Computer Society, Washington, DC, USA, pp 566–571.

Santos, N., Gummadi, K.P. & Rodrigues, R. (2009), "Towards Trusted Cloud Computing", In *Proceedings of the 2009 conference on Hot topics in cloud computing*, San Diego, California. USENIX Association Berkeley, CA, USA

Zhang, F., Huang, Y., Wang, H., Chen, H. & Zang, B. (2008), "PALM: Security Preserving VMLive Migration for Systems with VMM-enforced Protection", In *Trusted Infrastructure Technologies Conference, 2008*. APTC'08, Third AsiaPacific. IEEE Computer Society, Washington, DC, USA, pp 9–18.

Wei, J., Zhang, X., Ammons, G., Bala, V. & Ning, P. (2009), "Managing Security of virtual machine images in a Cloud environment", In *Proceedings of the 2009 ACM workshop on Cloud Computing Security*. ACM New York, NY, USA, pp 91–96.

Morsy, M.A., Grundy, J. & Müller, I. (2010), "An analysis of the Cloud Computing

Security problem", In *Proceedings of APSEC 2010 Cloud Workshop,* APSEC, Sydney, Australia

Wang, C., Wang, Q., Ren, K. & Lou, W. (2009), "Ensuring data Storage Security in Cloud Computing", In: *The 17th International workshop on quality of service*. IEEE Computer Society, Washington, DC, USA, pp 1–9.

OWASP, (2010), "The Ten most critical Web application Security risks", https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project

Jasti, A., Shah, P., Nagaraj, R. & Pendse, R. (2010), "Security in multi-tenancy cloud", In IEEE *International Carnahan Conference on Security Technology (ICCST)*, KS, USA, IEEE Computer Society, Washington, DC, USA, pp 35–41.

Reuben, J.S. (2007), "A survey on virtual machine Security," *Seminar on Network Security*

Xiao, S. & Gong, W. (2010), "Mobility Can help: protect tenant identity with dynamic credential", In *Eleventh International conference on Mobile data Management (MDM)*. IEEE Computer Society, Washington, DC, USA, pp 378–380.

Cloud Security Alliance. (2012), "SecaaS implementation guidance, category 1: identity and Access management", https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf.

Fong, E. & Okun, V. (2007), "Web application scanners: definitions and functions", In *Proceedings of the 40th annual Hawaii International conference on system sciences*, IEEE Computer Society, Washington, DC, USA.

Wang, Z. & Jiang, X. (2010), "Hyper-Safe: a lightweight approach to provide lifetime hypervisor control-flow integrity", In *Proceedings of the IEEE symposium on Security and privacy*. IEEE Computer Society, Washington, DC, USA, pp 380–395.

Han-zhang, W. & Liu-sheng, H. (2010), "An improved trusted cloud computing platform model based on DAA and privacy CA scheme", In *International Conference on Computer Application and System Modeling (ICCASM)*, IEEE Computer, Society, Washington, DC, USA, Vol13, pp13–33

Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., Valdez, E., Perez, R., Schildhauer W. & Srinivasan, D. (2008), “TVDc: managing Security in the trusted virtual datacenter”, *SIGOPS Oper*. Syst. Rev, Vol. 42, pp. 40–47.

Berger, S., Cáceres, R., Goldman, K., Pendarakis, D., Perez, R., Rao, J.R., Rom, E., Sailer, R., Schildhauer, W., Srinivasan, D., Tal, S., &Valdez, E. (2009), “Security for the Cloud infrastructure: trusted virtual data center implementation”, *IBM* J Res Dev Vol. 53, pp. 560–57.