Crossref Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

An Analysis of Security Issues in Cloud Computing

Onwodi, G.
Department of Computer Science
National Open University of Nigeria
Abuja, FCT, Nigeria
E-mail: gonwodi@noun.edu.ng

ABSTRACT

Our previous work and that of others was a systematic review of the existing literature regarding security in Cloud Computing was done not only to summarize the existing vulnerabilities and threats concerning this issue but also to identify and analyze the current state and most important security issues for Cloud Computing. Our focus was to identify the most relevant issues in Cloud Computing which consider vulnerabilities, threats, risks, requirements and solutions of security for Cloud Computing. In this paper we relate vulnerabilities and threats with possible solutions and provide an analysis as well as mitigating techniques based on our experiments and findings.

Keywords: Framework, Deployment, National Identification Number (NIN), Patients, Health, Emergencies, Healthcare.

Journal Reference Format:

Onwodi , G. (2019): An Analysis of Security Issues in Cloud Computing. Journal of Behavioural Informatics, Social-Cultural and Development Research. Vol. 5 . No. 4, Pp 1-14 www.isteams/behavioralinformaticsjournal. Article DOI No - dx.doi.org/10.22624/AIMS/BHI/V5N4P1

1. INTRODUCTION

Salient issues that has been identified as challenges in the cloud computing research environments include focus of implementation on Platform as a service and Software as a service leaving Infrastructure as a service behind. Other papers also concentrated on data Confidentiality without taking into account Integrity, non-repudiation and authenticity. Few works in literature were theoretical based meaning actual practical implementation was not done. In other papers, though the technique proposed seams reliable, but it looks weird, complicated and cumbersome to implement. Some proposed techniques were also not experimentally validated like the Access Control and Data Confidentiality (ACDC)

1.1 Selection of Sources

The selection criteria through which we evaluated study sources was based on the research experience of the authors of this work, and in order to select these sources we have considered certain constraints: studies included in the selected sources must be written in English and these sources must be web-available. The following list of sources has been considered: ScienceDirect, ACM digital library, IEEE digital library, Scholar Google and DBLP. Later, the experts will refine the results and will include important works that had not been recovered in these sources and will update these work taking into account other constraints such as impact factor, received cites, important journals, renowned authors, etc. Once the sources had been defined, it was necessary to describe the process and the criteria for study selection and evaluation. The inclusion and exclusion criteria of this study were based on the research question. We therefore established that the studies must contain issues and topics which consider security on Cloud Computing, and that these studies must describe threats, vulnerabilities, countermeasures, and risks.

Crossref Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

2. REVIEW EXECUTION

During this phase, the search in the defined sources must be executed and the obtained studies must be evaluated according to the established criteria. After executing the search chain on the selected sources we obtained a set of about 120 results which were filtered with the inclusion criteria to give a set of about 40 relevant studies. This set of relevant studies was again filtered with the exclusion criteria to give a set of studies which corresponds with 15 primary proposals [4][6][10][16][17][18][19][20][21][22][23][24][25][26][27].

3. RESULTS AND DISCUSSION

The results of the systematic review are summarized in
Table **1** which shows a summary of the topics and concepts considered for each approach.

Table 1. Summary of the topics considered in each approach

Topics / References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Vulnerabilities		X		X	X	X	X	X	X			X			X
Threats		X		X	X	X	X	X	X	X	X	X	X	X	X
Mechanisms/Recommendations	X			X		X		X				X	X	X	X
Security Standards							X			X					
Data Security	X		X				X		X		X		X		X
Trust			X								X		X	X	X
Security Requirements	X		X						X		X			X	X
SaaS, PaaS, IaaS Security					X				X			X			

Crossref Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

As it is shown in
Table **1**, most of the approaches discussed identify, classify, analyze, and list a number of vulnerabilities and threats focused on Cloud Computing. The studies analyze the risks and threats, often give recommendations on how they can be avoided or covered, resulting in a direct relationship between vulnerability or threats and possible solutions and mechanisms to solve them. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other issues related to security in the Cloud such as the data security, trust, or security recommendations and mechanisms for any of the problems encountered in these environments.

4. ANALYSIS OF SECURITY ISSUES IN CLOUD COMPUTING

We systematically analyze now existing security vulnerabilities and threats of Cloud Computing. For each vulnerability and threat, we identify what cloud service model or models are affected by these security problems.

Table 2 presents an analysis of vulnerabilities in Cloud Computing. This analysis offers a brief description of the vulnerabilities, and indicates what cloud service models (SPI) can be affected by them. For this analysis, we focus mainly on technology-based vulnerabilities; however, there are other vulnerabilities that are common to any organization, but they have to be taken in consideration since they can negatively impact the security of the cloud and its underlying platform. Some of these vulnerabilities are the following:

- Lack of employee screening and poor hiring practices [16] – some cloud providers may not perform background screening of their employees or providers. Privileged users such as cloud administrators usually have unlimited access to the cloud data.
- Lack of customer background checks – most cloud providers do not check their customer's background, and almost anyone can open an account with a valid credit card and email. Apocryphal accounts can let attackers perform any malicious activity without being identified [16].
- Lack of security education – people continue to be a weak point in information security [53]. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users.

Cloud Computing leverages many existing technologies such as web services, web browsers, and virtualization, which contributes to the evolution of cloud environments. Therefore, any vulnerability associated to these technologies also affects the cloud, and it can even have a significant impact.

Crossref Content Registered
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Table 2. Vulnerabilities in Cloud Computing

ID	Vulnerabilities	Description	Layer
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) [42]. The security of the cloud depends upon the security of these interfaces [16]. Some problems are: a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation	SPI
V02	Immature cloud APIs	Cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application [54].	SPI
V03	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning [17].	SPI
V04	Data-related vulnerabilities	a) Data can be collocated with unknown owners (competitors, or intruders) [36] b) Data may be located in different jurisdictions which have different laws [19][54][55] c) Incomplete data deletion – data cannot be completely removed [19][20][25][56] d) Data backup done by untrusted third-party providers [56][57] e) Information about the location of the data usually is unavailable or not disclosed to users [25] f) Data deduplication – a technique that stores only a copy of redundant data which may be not secured g) Data is often stored, processed, and transferred in clear plain text	SPI

Crossref Content Registered

Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

V05	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs [48][58][59] b) Unrestricted allocation and deallocation of resources with VMs [57] c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [42][44] d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility [12], which may lead to data leakage e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [44], but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography [58])	I
V06	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories [24] b) VM images are not able to be patched since they are dormant artifacts [44]	I
V07	Vulnerabilities in Hypervisors	a) Complex hypervisor code [60] b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	I
V08	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [51]	I

Table 3 presents an overview of threats in Cloud Computing. Like

Table 2 it also describes the threats that are related to the technology used in cloud environments, and it indicates what cloud service models are exposed to these threats. We put more emphasis on threats that are associated with data being stored and processed remotely, sharing resources and the usage of virtualization. From

Crossref Content Registered
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Table 2, we can conclude that data storage and virtualization are the most critical and an attack to them can do the most harm. Attacks to lower layers have more impact to the other layers.

Table 3. Threats in Cloud Computing

ID	Threats	Description	Layer
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [16].	SPI
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [17][25][10].	SPI
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [16][17][20][58].	SPI
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [20][32]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S
T06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [24][61].	I
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e by exploting some hypervisor vulnerability) [17][43]	I
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [20].	I
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [42] b) Transfer a VM to an untrusted host [44] c) Create and migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [45][51].	I

Crossref Content Registered

Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

The relationship between threats and vulnerabilities is illustrated in Table 4, which describes how a threat can take advantage of some vulnerability to compromise the system. The goal of this analysis is also to identify some existing defenses that can defeat these threats. This information can be expressed in a more detailed way using misuse patterns [62]. Misuse patterns describe how a misuse is performed from the point of view of the attacker. For instance, in threat T10, an attacker can read or tamper with the contents of the VM state files during live migration.
This can be possible because VM migration transfer the data over network channels that are often insecure, such as the Internet. Insecure VM migration can be mitigated by the following proposed techniques: TCCP [63] provides confidential execution of VMs and secure migration operations as well. PALM [64] proposes a secure migration system that provides VM live migration capabilities under the condition that a VMM-protected system is present and active. Threat 11 is another cloud threat where an attacker creates malicious VM image containing any type of virus or malware. This threat is feasible because any legitimate user can create a VM image and publish it on the provider's repository where other users can retrieve them. If the malicious VM image contains malware, it will infect other VMs instantiated with this malicious VM image. In order to overcome this threat, an image management system was proposed, Mirage [49]. It provides the following security management features: access control framework, image filters, provenance tracking system, and repository maintenance services.

Table 4. Relationships between Threats, Vulnerabilities, and Countermeasures

Threat	Vulnerabilities	Incidents	Countermeasures
T01	V01	An attacker can use the victim's account to get access to the target's resources.	Identity and Access Management Guidance [65] Dynamic credential [66]
T02	V04a, V04c	Data from hard drives that are shared by several customers cannot be completely removed.	Specify destruction strategies on Service-level Agreements (SLAs)
T03	V01, V04a, V04c, V04d, V04f, V05a-g, V06a, V08	Authors in [58] illustrated the steps necessary to gain confidential information from other VMs co-located in the same server as the attacker. Side channel [67]	FRS techniques [68] Digital Signatures [69] Encryption [67] Homomorphic encryption [70]
T04	V01, V03	An attacker can request more computational resources, so other legal users are not able to get additional capacity.	Cloud providers can force policies to offer limited computational resources
T05	V01, V02	Some examples are described in [32] such as SQL, command injection, and cross-site scripting	Web application scanners [71]
T06	V07a, V07b	A zero-day exploit in the HyperVM virtualization application that destroyed about 100,000 websites [72]	HyperSafe [60] TCCP (Trusted Cloud Computing Platform) [63] TVDc (Trusted Virtual Datacenter) [73][74]
T07	V05b, V07b	[75] presents a study that demonstrates security flaws in most virtual machines monitors	
T08	V06a, V06b	An attacker can create a VM image containing malware and publish it in a public repository.	Mirage [49]

Crossref Content Registered
Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

T09	V05d	[76] has empirically showed attacks against the migration functionality of the latest version of the Xen and VMware virtualization products.	PALM [64] TCCP [63] VNSS [52]
T10	V08	Sniffing and spoofing virtual networks [51]	Virtual network framework based on Xen network modes: "bridged" and "routed" [51]

Countermeasures
In this section, we provide a brief description of each countermeasure mentioned before, except for threats T02 and T07.

Countermeasures for T01: Account or service hijacking
Identity and Access Management Guidance: Cloud Security Alliance (CSA) is a non-profit organization that promotes the use of best practices in order to provide security in cloud environments. CSA has issued an Identity and Access Management Guidance [65] which provides a list of recommended best practiced to assure identities and secure access management. This report includes centralized directory, access management, identity management, role-based access control, user access certifications, privileged user and access management, separation of duties, and identity and access reporting.

Dynamic Credentials: [66] presents an algorithm to create dynamic credentials for mobile cloud computing systems. The dynamic credential changes its value once a user changes its location or when he has exchanged a certain number of data packets.

Countermeasures for T03: Data Leakage
Fragmentation-redundancy-scattering (FRS) technique [68]: This technique aims to provide intrusion tolerance and, in consequence, secure storage. This technique consists in first breaking down sensitive data into insignificant fragments, so any fragment does not have any significant information by itself. Then, fragments are scattered in a redundant fashion across different sites of the distributed system.

Digital Signatures: [69] proposes to secure data using digital signature with RSA algorithm while data is being transferred over the Internet. They claimed that RSA is the most recognizable algorithm, and it can be used to protect data in cloud environments.

Homomorphic encryption: The three basic operations for cloud data are transfer, store, and process. Encryption techniques can be used to secure data while it is being transferred in and out of the cloud or stored in the provider's premises. Cloud providers have to decrypt cipher data in order to process it, which raises privacy concerns.

In [70], they propose a method based on the application of fully homomorphic encryption to the security of clouds. Fully homomorphic encryption allows performing arbitrary computation on ciphertexts without being decrypted. Current homomorphic encryption schemes support limited number of homomorphic operations such as addition and multiplication. The authors in [77] provided some real-world cloud applications where some basic homomorphic operations are needed. However, it requires a huge processing power which may impact on user response time and power consumption.

Encryption: Encryption techniques have been used for long time to secure sensitive data. Sending or storing encrypted data in the cloud will ensure that data is secure. However, it is true assuming that the encryption algorithms are strong. There are some well-known encryption schemes such as AES (Advanced Encryption Standard). Also, SSL technology can be used to protect data while it is in transit. Moreover, [67] describes that encryption can be used to stop side channel attacks on cloud storage de-duplication, but it may lead to offline dictionary attacks reveling personal keys.

Countermeasures for T05: Customer Data Manipulation

Web application scanners: Web applications can be an easy target because they are exposed to the public including potential attackers. Web application scanners [71] is a program which scans web applications through the web front-end in order to identify security vulnerabilities. There are also other web application security tools such as web application firewall. Web application firewall routes all web traffic through the web application firewall which inspects specific threats.

Countermeasures for T06: VM Escape

HyperSafe [60]: It is an approach that provides hypervisor control-flow integrity. HyperSafe's goal is to protect type I hypervisors using two techniques: non-bypassable memory lockdown which protects write-protected memory pages from being modified, and restricted pointed indexing that converts control data into pointer indexes. In order to evaluate the effectiveness of this approach, they have conducted four types of attacks such as modify the hypervisor code, execute the injected code, modify the page table, and tamper from a return table. They concluded that HyperSafe successfully prevented all these attacks, and that the performance overhead is low.

Trusted Cloud Computing Platform: TCCP [63] enables providers to offer closed box execution environments, and allows users to determine if the environment is secure before launching their VMs. The TCCP adds two fundamental elements: a trusted virtual machine monitor (TVMM) and a trusted coordinator (TC). The TC manages a set of trusted nodes that run TVMMs, and it is maintained but a trusted third party. The TC participates in the process of launching or migrating a VM, which verifies that a VM is running in a trusted platform. The authors in [78] claimed that TCCP has a significant downside due to the fact that all the transactions have to verify with the TC which creates an overload. They proposed to use Direct Anonymous Attestation (DAA) and Privacy CA scheme to tackle this issue.

Trusted Virtual Datacenter: TVDc [73][74] insures isolation and integrity in cloud environments. It groups virtual machines that have common objectives into workloads named Trusted Virtual Domains (TVDs). TVDc provides isolation between workloads by enforcing mandatory access control, hypervisor-based isolation, and protected communication channels such as VLANs. TVDc provides integrity by employing load-time attestation mechanism to verify the integrity of the system.

Countermeasures for T08: Malicious Virtual Machine Creation

Mirage: In [49], the authors propose a virtual machine image management system in a cloud computing environments. This approach includes the following security features: access control framework, image filters, a provenance tracking, and repository maintenance services. However, one limitation of this approach is that filters may not be able to scan all malware or remove all the sensitive data from the images. Also, running these filters may raise privacy concerns because they have access to the content of the images which can contain customer's confidential data.

Countermeasures for T09: Insecure Virtual Machine Migration

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Protection Aegis for Live Migration of VMs (PALM): [64] proposes a secure live migration framework that preserves integrity and privacy protection during and after migration. The prototype of the system was implemented based on Xen and GNU Linux, and the results of the evaluation showed that this scheme only adds slight downtime and migration time due to encryption and decryption. VNSS: [52] proposes a security framework that customizes security policies for each virtual machine, and it provides continuous protection thorough virtual machine live migration. They implemented a prototype system based on Xen hypervisors using stateful firewall technologies and userspace tools such as iptables, xm commands program and conntrack-tools. The authors conducted some experiments to evaluate their framework, and the results revealed that the security policies are in place throughout live migration.

Countermeasures for T010: Sniffing/Spoofing virtual networks

Virtual Network Security: Wu and et al [51] presents a virtual network framework that secures the communication among virtual machines. This framework is based on Xen which offers two configuration modes for virtual networks: "bridged" and "routed". The virtual network model is composed of three layers: routing layers, firewall, and shared networks, which can prevent VMs from sniffing and spoofing. An evaluation of this approach was not performed when this publication was published.

Furthermore, web services are the largest implementation technology in cloud environments. However, web services also lead to several challenges that need to be addressed. Security web services standards describe how to secure communication between applications through integrity, confidentiality, authentication and authorization. There are several security standard specifications [79] such as Security Assertion Markup Language (SAML), WS-Security, Extensible Access Control Markup (XACML), XML Digital Signature, XML Encryption, Key Management Specification (XKMS), WS-Federation, WS-Secure Conversation, WS-Security Policy and WS-Trust. The NIST Cloud Computing Standards Roadmap Working Group has gathered high level standards that are relevant for Cloud Computing.

5. CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.

Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

WORKS CONSULTED/REFERENCED

[1] Gartner Inc., "Gartner Identifies the Top 10 Strategic Technologies for 2011." [Online]. Available: http://www.gartner.com/it/page.jsp?id=1454221. [Accessed: 15-Jul-2011].

[2] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. Ye, and N. Tang, "Cloud Computing: A Statistics Aspect of Users," in *First International Conference on Cloud Computing (CloudCom)*, Beijing, China, 2009, pp. 347–358.

[3] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud Computing Research and Development Trend," in *Second International Conference on Future Networks (ICFN '10)*, Sanya, Hainan, China, 2010, pp. 93 –97.

[4] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0." 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] A. Marinos and G. Briscoe, "Community Cloud Computing," in *1st International Conference on Cloud Computing (CloudCom)*, Beijing, China, 2009.

[6] Centre for the Protection of National Infrastructure, "Information Security Briefing 01/2010 Cloud Computing," Mar-2010. Available: http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf

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

[8] KPMG, "From Hype to Future: KPMG's 2010 Cloud Computing Survey." 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291

[9] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina, "Security Analysis in the Migration to Cloud Environments," *Future Internet*, vol. 4, no. 2, pp. 469–487, May 2012.

[10] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy*. O'Reilly Media, Inc., 2009.

[11] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment," in *Proceedings of the 1st International Conference on Cloud Computing*, Beijing, China, 2009, pp. 69–79.

[12] J. W. Rittinghouse and J. F. Ransome, "Security in the Cloud," in *Cloud Computing: Implementation, Management, and Security*, CRC Press, 2009.

[13] B. Kitchenham, "Procedures for Perfoming Systematic Review," Software Engineering Group, Department of Computer Scinece Keele University, United Kingdom and Empirical Software Engineering, National ICT Australia Ltd., Australia, TR/SE-0401, 2004.

[14] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering. Version 2.3," University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Conputer Science), UK, 2007.

[15] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *Journal of Systems and Software*, vol. 80, no. 4, pp. 571–583, 2007.

[16] Cloud Security Alliance, "Top Threats to Cloud Computing V1.0." 2010. Available: https://cloudsecurityalliance.org/research/top-threats/

[17] ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security." 2009. Available: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[18] K. Dahbur, B. Mohammad, and A. B. Tarakji, "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, 2011, pp. 1–6.
[19] L. Ertaul, S. Singhal, and S. Gökay, "Security Challenges in Cloud Computing," in *Proceedings of the 2010 International Conference on Security and Management SAM'10*, Las Vegas, US, 2010, pp. 36–42.
[20] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," *IEEE Security Privacy*, vol. 9, no. 2, pp. 50 –57, 2011.
[21] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011.
[22] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," in *IEEE International Conference on Cloud Computing (CLOUD '09)*, 2009, pp. 109 –116.
[23] C. Onwubiko, "Security Issues to Cloud Computing," in *Cloud Computing: Principles, Systems & Applications*, N. Antonopoulos and L. Gillam, Eds. Springer-Verlag, 2010.
[24] M. A. Morsy, J. Grundy, and I. Müller, "An Analysis of The Cloud Computing Security Problem," in *Proceedings of APSEC 2010 Cloud Workshop*, Sydney, Australia, 2010.
[25] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, Koloa, Kauai, HI, 2011, pp. 1–10.
[26] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.
[27] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," NIST, Special Publication 800-144, 2011.
[28] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Special Publication 800-145, Sep. 2011.
[29] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *Journal of Internet Services Applications*, vol. 1, no. 1, pp. 7–18, May 2010.
[30] J. Ju, Y. Wang, J. Fu, J. Wu, and Z. Lin, "Research on Key Technology in SaaS," in *International Conference on Intelligent Computing and Cognitive Informatics (ICICCI)*, 2010, pp. 384 –387.
[31] D. Owens, "Securing Elasticity in the Cloud," *Communications of the ACM*, vol. 53, no. 6, pp. 46–51, May-2010.
[32] OWASP, "The Ten Most Critical Web Application Security Risks." 2010. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[33] Y. Zhang, S. Liu, and X. Meng, "Towards high level SaaS maturity model: Methods and case study," in *Services Computing Conference. APSCC 2009. IEEE Asia-Pacific*, 2009, pp. 273 –278.
[34] F. Chong, G. Carraro, and R. Wolter, "Multi-Tenant Data Architecture," Jun-2006. [Online]. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx. [Accessed: 05-Jun-2011].
[35] C.-P. Bezemer and A. Zaidman, "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, 2010, pp. 88–92.
[36] J. Viega, "Cloud Computing and the Common Man," *Computer*, vol. 42, no. 8, pp. 106–108, Aug-2009.
[37] Cloud Security Alliance, "Security Guidance for Critical Areas of Mobile Computing." Nov-2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf

[38] C. Keene, "The Keene View on Cloud Computing," 18-Mar-2009. [Online]. Available: http://www.keeneview.com/2009/03/what-is-platform-as-service-paas.html. [Accessed: 16-Jul-2011].
[39] K. Xu, X. Zhang, M. Song, and J. Song, "Mobile Mashup: Architecture, Challenges and Suggestions," in *International Conference on Management and Service Science. MASS '09*, 2009, pp. 1 –4.
[40] R. Chandramouli and P. Mell, "State of security readiness," *Crossroads*, vol. 16, no. 3, pp. 23–25, Mar-2010.
[41] T. Jaeger and J. Schiffman, "Outlook: Cloudy with a Chance of Security Challenges and Improvements," *IEEE Security Privacy*, vol. 8, no. 1, pp. 77 –80, 2010.
[42] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a service security: Challenges and solutions," in *the 7th International Conference on Informatics and Systems (INFOS)*, 2010, pp. 1 –8.
[43] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2010, pp. 35 –41.
[44] T. Garfinkel and M. Rosenblum, "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, 2005, vol. 10, pp. 227–229.
[45] J. S. Reuben, "A survey on virtual machine security," *Seminar on Network Security*, 2007.
[46] K. Hashizume, N. Yoshioka, and E. B. Fernandez, "Three Misuse Patterns for Cloud Computing," in *Security Engineering for Cloud Computing: Approaches and Tools*, D. G. Rosado, D. Mellado, E. Fernandez-Medina, and M. Piattini, Eds. IGI Global, 2013, pp. 36–53.
[47] S. Venkatesha, "Survey of Virtual Machine Migration Techniques," 2009.
[48] P. Ranjith, P. Chandran, and S. Kaleeswaran, "On Covert Channels between Virtual Machines," *Journal in Computer Virology, Springer*, vol. 8, pp. 85–97, 2012.
[49] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 91–96.
[50] K. Owens, "Securing Virtual Compute Infrastructure in the Cloud." SAVVIS. Available: http://www.savvis.com/en-us/info_center/documents/hos-whitepaper-securingvirutalcomputeinfrastructureinthecloud.pdf
[51] H. Wu, Y. Ding, C. Winer, and L. Yao, "Network security for virtual machine in cloud computing," in *5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, 2010, pp. 18 –21.
[52] G. Xiaopeng, W. Sumei, and C. Xianqin, "VNSS: A network security sandbox for virtual computing environment," in *IEEE Youth Conference on Information Computing and Telecommunications (YC-ICT)*, 2010, pp. 395 –398.
[53] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *Proceedings of the 33rd International Convention MIPRO*, 2010, pp. 344 –349.
[54] S. Carlin and K. Curran, "Cloud Computing Security," *International Journal of Ambient Computing and Intelligence*, vol. 3, no. 1, pp. 38–46, 2011.
[55] A. Bisong and S. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Computing," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, no. 1, pp. 30–45, Jan. 2011.
[56] M. Townsend, "Managing a security program in a cloud computing environment," in *Information Security Curriculum Development Conference*, Kennesaw, Georgia, 2009, pp. 128–133.

[57] V. Winkler, *Securing the cloud: Cloud computer security techniques and tactics*. Elsevier Inc., 2011.

[58] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "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, 2009, pp. 199–212.

[59] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-VM side channels and their use to extract private keys," in *Proceedings of the 2012 ACM conference on Computer and communications security*, New York, NY, USA, 2012, pp. 305–316.

[60] Z. Wang and X. Jiang, "HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity," in Proceedings of the IEEE Symposium on Security and Privacy, 2010, pp. 380–395.

[61] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in Cloud Computing," in the 17th International Workshop on Quality of Service, 2009, pp. 1–9.

[62] E. B. Fernandez, N. Yoshioka, and H. Washizaki, "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, 2009, pp. 566 –571.

[63] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards Trusted Cloud Computing," in *Proceedings of the 2009 conference on Hot topics in cloud computing*, San Diego, California, 2009.

[64] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang, "PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection," in *Trusted Infrastructure Technologies Conference, 2008. APTC '08. Third Asia-Pacific*, 2008, pp. 9 –18.

[65] Cloud Security Alliance, "SecaaS Implementation Guidance, Category 1: Identity and Access Managament." 2012. Available: https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[66] S. Xiao and W. Gong, "Mobility Can Help: Protect User Identity with Dynamic Credential," in *Eleventh International Conference on Mobile Data Management (MDM)*, 2010, pp. 378 –380.

[67] D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Side Channels in Cloud Services: Deduplication in Cloud Storage," *IEEE Security Privacy*, vol. 8, no. 6, pp. 40 –47, 2010.

[68] J. Wylie, M. Bakkaloglu, V. Pandurangan, M. Bigrigg, S. Oguz, K. Tew, C. Williams, G. Ganger, and P. Khosla, "Selecting the right data distribution scheme for a survivable storage system," CMU-CS-01-120, May 2001.

[69] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," in *1st International Conference on Parallel Distributed and Grid Computing (PDGC)*, 2010, pp. 211 –216.

[70] M. Tebaa, S. El Hajji, and A. El Ghazi, "Homomorphic encryption method applied to Cloud Computing," in *National Days of Network Security and Systems (JNS2)*, 2012, pp. 86 –89.

[71] E. Fong and V. Okun, "Web Application Scanners: Definitions and Functions," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 2007.

[72] D. Goodin, "Webhost hack wipes out data for 100,000 sites," *The Register*, 08-Jun-2009. [Online]. Available: http://www.theregister.co.uk/2009/06/08/webhost_attack/. [Accessed: 02-Aug-2011].

[73] S. Berger, R. Cáceres, D. Pendarakis, R. Sailer, E. Valdez, R. Perez, W. Schildhauer, and D. Srinivasan, "TVDc: managing security in the trusted virtual datacenter," *SIGOPS Oper. Syst. Rev.*, vol. 42, no. 1, pp. 40–47, Jan. 2008.

[74] S. Berger, R. Cáceres, K. Goldman, D. Pendarakis, R. Perez, J. R. Rao, E. Rom, R. Sailer, W. Schildhauer, D. Srinivasan, S. Tal, and E. Valdez, "Security for the cloud infrastructure: trusted virtual data center implementation," *IBM Journal of Research and Development*, vol. 53, no. 4, pp. 560–571, Jul. 2009.

[75] T. Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments," in *CanSecWest Applied Security Conference*, Vancouver, 2007.

[76] J. Oberheide, E. Cooke, and F. Jahanian, "Empirical Exploitation of Live Virtual Machine Migration," in *Proceedings of BlackHat DC convention*, 2008.

[77] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011, pp. 113–124.

[78] W. Han-zhang and H. Liu-sheng, "An improved trusted cloud computing platform model based on DAA and privacy CA scheme," in *International Conference on Computer Application and System Modeling (ICCASM)*, 2010, vol. 13, pp. V13–33 –V13–39.

[79] E. B. Fernandez, O. Ajaj, I. Buckley, N. Delessy-Gassant, K. Hashizume, and M. M. Larrondo-Petrie, "A Survey of Patterns for Web Services Security and Reliability Standards," *Future Internet*, vol. 4, no. 2, pp. 430–450, Apr. 2012.