ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 4, 44-50 (2017)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Toward Confirming a Framework for Securing the Virtual Machine Image in Cloud Computing

Raid Khalid Hussein [1]*, Ahmed Alenezi [1, 2], Hany F.Atlam [1, 3], Mohammed Q Mohammed [4], Robert J. Walters [1], Gary B. Wills [1]

[1] *Electronic and Computer Science Dept., University of Southampton, SO17 1BJ, UK*

[2] *Dept. of Computer Science, Faculty of Computing and Information Technology, Northern Border University, 1321, Saudi Arabia*

[3] *Computer Science and Engineering Dept., Faculty of Electronic Engineering, Menoufia University, 32952, Egypt*

[4] *Dept. of Computer Science, University of Information technology and communication, Bagdad, Iraq.*

ARTICLE INFO

Article history:
Received: 04 March, 2017
Accepted: 11 April, 2017
Online: 24 April, 2017

Keywords:
Cloud Computing
Virtual Machine Image
Information Security
Virtualisation

ABSTRACT

The concept of cloud computing has arisen thanks to academic work in the fields of utility computing, distributed computing, virtualisation, and web services. By using cloud computing, which can be accessed from anywhere, newly-launched businesses can minimise their start-up costs. Among the most important notions when it comes to the construction of cloud computing is virtualisation. While this concept brings its own security risks, these risks are not necessarily related to the cloud. The main disadvantage of using cloud computing is linked to safety and security. This is because anybody which chooses to employ cloud computing will use someone else's hard disk and CPU in order to sort and store data. In cloud environments, a great deal of importance is placed on guaranteeing that the virtual machine image is safe and secure. Indeed, a previous study has put forth a framework with which to protect the virtual machine image in cloud computing. As such, the present study is primarily concerned with confirming this theoretical framework so as to ultimately secure the virtual machine image in cloud computing. This will be achieved by carrying out interviews with experts in the field of cloud security.

1 Introduction

Recent times have seen a sudden increase in the number of organisations adopting cloud computing; indeed, this growth has brought about a 21st-century computing paradigm. As a type of information technology, the cloud includes a number of internet-based commercial applications; these applications exist because of today's greater bandwidth, thus giving present-day users the chance to exploit the advantages offered by top-quality data services and application software. Being scalable in nature, cloud computing takes advantage of virtualisation to spread resources. For those who use the cloud, of particular importance is a resource base that houses numerous IT resources, the purpose of which is to distribute computing assignments that necessitate a substantial amount of processing capability. Surfers of the Web can easily ear-mark online storage space, which they can then use to safely store their data; indeed, they can also gain access to IT resources which they can employ to manage and sort their information according to their requirements. This paper builds on work which was originally presented at the IEEE International Conference on Smart Cloud 2016 [1].

Cloud computing itself gives rise to a number of security issues linked to resource scheduling, databases, virtualisation, load balancing and networks [2]. Numerous organisations are of the opinion that moving their sensitive data to central datacentres is fraught with danger. This scepticism stems from the fact that the management staff in charge of these datacentres might not be trustworthy [3]. Switching databases to a datacentre involves many security-related obstacles, e.g. access control issues, virtualisation vulnerability, integrity and confidentiality [4].

Among the most vital elements of cloud computing is virtualisation, which minimises the cost of hardware and supports techniques used for saving energy [4]. Virtualisation can be broken down into three types: application level virtualisation, operating system level virtualisation, and Virtual Machine Monitor (VMM)

* Raid Khalid Hussein, Flat 3 1 Alma road Southampton SO14 6UN, 00447466256351, Email: rkh2n14@soton.ac.uk

or hypervisor level virtualisation [5]. When one real-life machine is used to run two different virtual machines, this might affect data security, as these machines are not completely separated by the virtualisation. Moreover, the Virtual Machine Monitor, or hypervisor, has control, but not complete control, over the host and its operating system (OS) [6].

Among the most important elements of cloud computing is multi-tenancy. Indeed, while this is thought to be one of the most beneficial components of cloud computing, it nevertheless poses a threat to security, due to the fact that it spreads infrastructure resources across different customers [7]. The hardware layer of cloud computing contains no absolute separation, and thus various breaches can materialise, such as unauthorised viewing, data leakage, and theft of sensitive or confidential data [8].

Previous studies have put forth a security framework which can be used to protect the Virtual Machine (VM) image in cloud computing [1]. The present paper details exactly how the conceptual framework has been confirmed through interviews with experts in the field of cloud security. Indeed, this paper is broken down into the following sections: Section 2 summarises the concept of cloud computing, Section 3 explores concerns related to cloud security, Section 4 examines related work, Section 5 details the research methodology used, Section 6 presents the results and findings of the research, which are subsequently discussed in Section 7, and Section 8 puts forth conclusions and outlines plans for additional work in the future.

2 Cloud Computing

Recent times have witnessed the rapid development of hardware, the introduction of distributed computing, and the tremendous success of internet technologies. All of these factors have made computing resources more powerful, cheaper and more readily available than ever before [9]. Current developments in hardware and software have ushered in a new computing model called cloud computing. In the cloud, computing resources are delivered to the users as services, just like public utilities. Consumers of these resources can contract for the services based on their needs, while the services can be scaled up or down as necessary. The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling 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" [10].

3 Cloud Security Issues

As concluded by the NIST, security is the primary concern when it comes to delays in adopting cloud computing [11]. This is because cloud computing has certain vulnerabilities which can potentially affect the major foundations of information security. These vulnerabilities are essentially weak points of the system that could be taken advantage of by someone attempting to infiltrate the cloud. Indeed, with the right tools, a person could gain illegal access to these resources. When talking about a threat, the basic premise is that an attacker could use unlawful means to gain access to such resources [12]. Figure 1 summarises safety and security concerns which are found in different areas of cloud computing. When it comes to virtualisation, resources can be grouped together or spread throughout numerous environments, namely Virtual Machines (VM). A VM is defined as "A way of making a physical computer function as if it were two or more computers where each non-physical or virtualized computer (machine) is provided with the same basic architecture as that of a generic physical computer.

Application level issues	Network level issues	Data Storage level issues
Authentication and access control level		Trusted level issues
Virtualisation level Issues		
VM isolation	VM rollback	VM escape
VM migration	VM sprawl	VM image sharing

Figure 1 Security issues in Cloud Computing

Virtualization technology therefore allows the installation of an operating system on hardware that does not really exist" [14]. An OS is hosted by the VM [15], with the former representing the virtualisation element which makes it possible for a guest OS to run on a host computer [13].

A very handy feature of cloud computing, multi-tenancy can be defined as "a property of a system where multiple customers, so-called tenants, transparently share the system's resources, such as services, applications, databases, or hardware, with the aim of lowering costs, while still being able to exclusively configure the system to the needs of the tenant" [16]. Multi-tenancy can be broken down into two categories: multiple instance and native multi-tenancy. With regards multiple instance tenancy, each tenant benefits from the services of a dedicated application instance from a shared OS, hardware and middleware server in a hosted environment. However, in relation to native multi-tenancy, one instance of a program can provide service to several tenants across numerous hosting resources. When looking at the Software as a Service (SaaS) model, it is clear that multi-tenancy can be linked to four varied software layers: the virtual layer, the application layer, the OS layer, and the middleware layer [17].

With regards a multi-tenancy virtualised environment, every user is assigned a VM that plays host to a guest OS. It is possible that VMs belonging to different users will have identical real-life resources as a result of resource pooling. The purpose of the VMM is to orchestrate the VMs and makes it possible for the numerous OS instances to function on the same physical hardware [18]. With regards the multi-tenancy virtualised environment, certain security elements have come into focus, such as VM isolation, which pertains to guaranteeing that VMs that function on identical physical hardware are kept apart from one another.

VMs may be transported (migrated) to various real-life hosts – a move which often occurs because of maintenance, load balancing, and fault tolerance. It is possible that a VM which has been transported may be infiltrated by an attacker and redistributed to an infected VMM or unsteady server [19]. If essential, it is possible to roll back VMs to a former state. This facility gives the user a great deal of flexibility, but also gives rise to security concerns; this is because, when it happens, the result may be a VM being exposed once more to a vulnerability that had previously been resolved [12]. In addition, it is plausible for a VM to escape

from the control of the VVM. This kind of VM can give an attacker the ability to access additional VMs in the same hardware, or disable the VMM altogether [20]. Another issue, known as VM sprawl, comes about when numerous VMs are being hosted by a system, but the majority of said VMs are serving no purpose. This situation can lead to a significant waste of the resources found within the host machine [21].

Among the most common threats to the security of the cloud is VM image sharing, simply because the image represents the initial state for new VM instances [18]. Taking into consideration both confidentiality and integrity is vital if the VM image is to be secured; this is due to the fact that, if an attacker can gain unauthorised access and is malicious, then said attacker can delete, modify, and alter administrator passwords, or formulate malicious VM instances. Another risk which certainly exists is non-compliance and running unlicensed software [5].

4 Related Work

It is certainly true that virtualisation is vital when it comes to cloud computing; however, it is also accompanied by various security concerns. Of these issues, one of the most important is VM image sharing, simply because the VM image is used to initialise new VMs. Numerous studies have focused on ways in which to secure the VM image. The Image Management System (IMS) addresses four security requirements: outdated software detection, access control, left owners' data removal, and malware protection. With this said, however, no attention is paid to privacy and integrity [22]. The Encrypted Virtual Disk Images in Cloud (EVDIC) tool looks at integrity, privacy, and access control; it does so by means of encrypting the VM image when it finishes. However, it is unable to detect outdated software or leftover owners' data removal [24]. Among other techniques to have been proposed are those used to check for software updates in the VM image [24, 25, 26]. These techniques are specifically utilised to search for software updates in the VM image, but do not take into account additional security requirements. Of these past studies, none have addressed every single security requirement necessary to safeguard the VM image in cloud computing. Hence, there is the need for a new method with which to secure all elements of the cloud-based VM image.

5 Research Methodology

This section describes the research methodology which was used to confirm the framework and identify additional requirements which are necessary in order to secure cloud computing VM images, as shown in [1]. The initial framework, shown in Figure 2, was derived from the literature review. A review by cloud security experts was carried out to explore the proposed framework and establish if any security requirements are missing.

The method used was an expert review, which is a qualitative approach. This form of research is used to gain an understanding of underlying reasons, opinions and motivations in the research area. It does not use statistical procedures or other means of quantification [27]. For this work, interviews were conducted with people who have in-depth knowledge of the subject under study [28], although the method can also use group discussions or video conferencing. This use of interviews permits the collection of valid and reliable data that are relevant to the research and its objectives [29]. The sample size requirements are based on an heuristic evaluation, which often uses between three and five experts [30].

In order to achieve the aims of the present study, interviews were carried out with a total of eight UK-based experts in the field of cloud security. The semi-structured interviews consisted of a set of questions that had been prepared in advance. The use of semi-structured interviews means that, by also employing an exploratory study, it is possible to understand the exact nature of the topic at hand [31]. All of the respondents were selected as a result of their expertise in the area under study.

Pilot-testing for the interview questions involved three security research fellows at the University of Southampton. Following this pre-test, the decision was taken to ask the respondents open questions regarding the importance of every security requirement and framework factor; this choice was a reversal of the original plan to have respondents fill out a table indicating the importance of said requirements and factors [28, 29]. Throughout the interviews, experts were expected to respond in their own words, with no possible answers suggested by the interviewer [33]. Interviews either took the form of face-to-face interaction, or online Skype calls [34]; said interviews were recorded using an audio recorder or by means of manual note-taking.

Prior to commencing the interviews, every expert was required to sign a consent form after thoroughly reviewing the participant information sheet, which presented all the necessary information, including the terms and conditions of the research [32]. This study was approved by The University of Southampton Ethics Committee (reference number 22876).

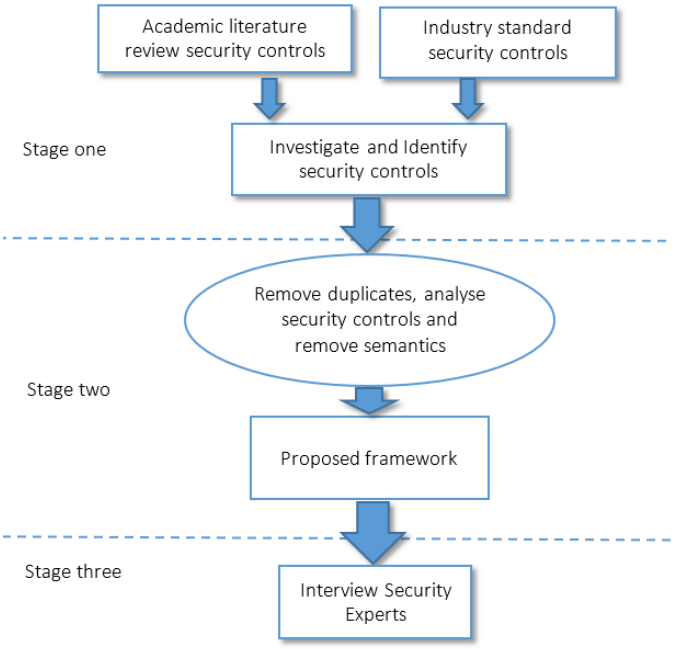

Figure 2. Framework development process to secure the VM image in cloud computing

6 Results and findings

The results are divided into two sections: Demographic Information and Qualitative Data.

6.1 Demographic Information

The data were collected from eight cloud security experts in the United Kingdom, all of whom were from different organisations.

All the interviewees had at least three years' experience dealing with cloud security and virtualisation issues, and thus all had the ability to understand and explain current security situations and trends. The interviews were conducted either face-to-face or via Skype video conferencing [34] between July and December 2016. The audio conferencing was recorded using the QuickTime recorder application. Face-to-face interviews were recorded using the Apple voice memory application. Details of the experts used in this study are presented in Table 1.

Table 1: Cloud security experts' attributes used to validate the framework

Code	Job Description	Experience (years)	Cloud involvement
A	Director of the IBM Institute of Advanced Security in Europe	17	Cloud policy
B	Cloud Systems Administrator	10	Cloud Security Architect
C	Cloud Systems Implementer	4	Cloud System Administrator
D	Cloud Security Administrator	6	Cloud System Administrator
E	Cloud Security Consultant	5	Direct advisory involvement with cloud implementation
F	Cloud Security Consultancy	4	Direct advisory involvement with cloud implementation
G	Cloud Security Consultancy	7	Cloud Security Consultant
H	Cloud Security Officer	4	Link between Cloud deployment & security policies

6.2 Qualitative Data

The purpose of the expert interviews was to review the identified security requirements and establish if there are more security requirements not included in the framework. Before interview questions were asked, each expert was given a brief background of the research area and the aim of the study. After the research had been outlined, five open-ended question were put to the experts [35]. The first question asked the cloud security experts about the importance of the identified security requirements. The experts gave an opinion about each of the requirements based on their expertise in the field. With regards the next question, the identified security requirements were defined according to the context of the study. The experts were asked to explain the security requirements in the context of securing the VM image. In the subsequent questions, they were asked whether there are more security requirements not mentioned in the framework and how they felt about the possibility of overlap or related factors. Finally, the experts were asked if they have any other methodologies or approaches to secure the VM image.

Most of the experts felt that the security requirements identified in the framework are essential when it comes to securing the VM image in cloud computing. The identified security requirements are: privacy, integrity, availability, accountability, regulatory compliance, encryption, authorisation, authentication, out-dated software detection, malware protection, left owner' data removal, auditing and trust. However, Expert B felt that regulatory compliance is irrelevant to the designed framework, while Expert D opined that privacy and trust are not necessary when it comes to securing the VM image.

Some of the experts did not agree fully with the definitions of the security requirements that are discussed in [1], and added additional details to the definitions. Most of the interviewed experts agreed with the provided definition of privacy. However, Experts B, D and E only partially agreed with this definition and added more details. Expert B was of the opinion that privacy is related to the data rather than the VM image itself. He stated that "Privacy is about saved data not the VM image. The VM image should be securely built". Moreover, Expert D believed that building a secure layer is sufficient to ensure the required security for the VM image. He said that "Privacy is the layer where you define or set policies to secure the VM image". In contrast, Expert E thought that different mechanisms, such as regulatory compliance, are required to achieve privacy. He opined that "There are other mechanisms used to ensure privacy like regulatory compliance".

The majority of the experts agreed with the provided definition of auditing. However, Experts A and C only agreed partially with this definition. Expert A believed that auditing is about keeping track of the client's access usage. He said, "Auditing is about recording the usage/access of the user to the VM image". Expert C thought that auditing is related to storing processes that are performed by the client during the access session to understand what is happening in the system. He stated that "Audit is taking a review of a system and an ongoing process to find out what is happening to something".

All the interviewed experts agreed with the provided definition of accountability and regulatory compliance. However, Expert E felt that internal compliance is essential and should be considered. He posited that "Internal compliance to reach a set of standards can also be considered". In contrast, Expert B believed that regulatory compliance indirectly affects the security of VM. He was of the opinion that keeping the operating system and anti-virus up-to-date is necessary to ensure the regulatory compliance of the VM image. He stated that "Regulatory compliance does not directly refer to VM image but, it does so indirectly as it requires Operating System and anti-virus to be to up-to-date".

Most of the experts agreed with the provided definition of encryption. However, Expert G only agreed partially with the definition. He felt that authorised devices also needed to be considered. All the interviewed experts agreed completely with the provided definitions of authentication, integrity and availability. They felt that there is no need for more details related to its definition. Most of the interviewed experts agreed with the provided definition of authorisation. However, Expert A disagreed. He felt that setting the appropriate policies is the essential element when it comes to ensuring efficient authorisation. He stated that "Administrator typically sets the policies. They define the policies for authorisation but, the process of the authorisation is automated as it is a large complicated process". Moreover, Expert G believed that authorisation is an automated process, thus meaning that the administrator is not dealing with checking users' rights. He stated that "Authorisation is usually driven out of permissions assigned to users or groups, not by administrations checking customers' right". Many of the experts agreed with the provided definition of out-dated software detection. Conversely, Expert G disagreed with this definition to some extent. He asked, "What about the software version of the virtual hardware in the VM image itself?". Expert A also disagreed with this definition. He believed that the software update should be against the versions of that particular software. Most of the experts

supported the provided definition of malware protection. With this said, however, Expert A only agreed with this definition to a certain extent, adding that malware should be detected, blocked and then removed from the VM image. Moreover, Expert E disagreed, to some extent, with this definition, but added that "It is a protective measure for detection, not a user removal. Proactive protection as well as reactive".

The majority of the experts agreed with the provided definition of left-over data removal. However, Expert A mentioned that personal data needed to be destroyed. Many of the interviewed experts supported the definition of trust. However, Expert A disagreed, to some extent, with this definition, though he mentioned that trust is all about confidence and assurance in using the VM image. He also mentioned that integrity of the VM image is important and thus the VM image should not include bugs, defects or malware.

After conducting the interviews with the cloud security experts, the security requirements were reviewed and updated based on the context for securing the VM image in cloud computing. The definitions with which the interviewed experts agreed (as shown in Figure 3), are listed below:

- Privacy: Refers to a set of policies that is used mainly for securing the data within the VM image [36], and these policies must ensure that regulatory compliance is taken into consideration.
- Auditing: Relates to recording the usage or access of authorised users to VM image resources, which helps to secure the VM image. Audit is the systematic security review of the information related to an organisation and how well it conforms to a set of criteria [37].
- Accountability: This is a measure of the amount of information an authorised customer is using during his/her session. This includes the quantity of data and time which is used to set authorisation control [38].
- Regulatory compliance: This refers to conformity to rules such as policy, law, and specifications relevant to the business while an organisation is working on the goal they wish to achieve. Regulatory compliance sometimes does not refer to the VM image itself, although it does refer to the operating system and the need for anti-virus measures to be kept up to date. Internally, it represents the set of polices specific to the organisation or the project [39].
- Encryption: A technique used to secure the shared data used by authorised users and authorised devices in a shared environment. In information systems, encryption is achieved by converting the data to a form that can only be understood by authorised people [40].
- Authentication: The process of identifying the customer as one authorised to use the cloud service. This is achieved by comparing the file of authorised users' information in the database with credentials provided by the user [41].
- Authorisation: This refers to the set of polices assigned by the administrator, while the implementation of these polices is automated [42].
- Outdated software detection: Is the comparison of software updates against the set of software versions within the VM image [18].
- Malware protection: Is a protective measure to detect, block and remove malware from the VM image. It includes proactive as well as reactive protection [26].
- Leftover owner's data removal: A technique used to promptly remove authentication details, as well as personal and private data from the VM image [22].
- Trust: Is the confidence and assurance of using the VM image, which belongs to a certain provider. In reality, it is the confidence and assurance in the provider who provides the VM image. The integrity of the VM image is important, and so the VM image should not include bugs, defects or malware [43].
- Integrity: This means that information remains unaltered while it is stored or being transmitted, and can only be modified and deleted by authorised users [44].
- Availability: Availability means that information must be available when it is needed. Systems with high availability allow access to data all the time and prevent service disruptions due to hardware failure, system upgrades, power outages, power failure, and operating system or application problems [45].

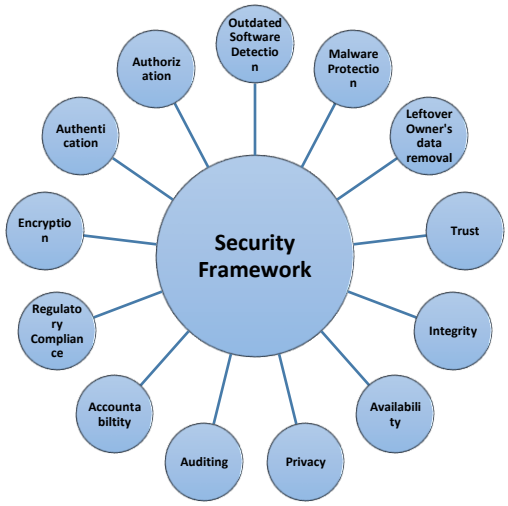

Figure 3. Security requirements agreed by security experts

All the experts agreed that the security framework designed to secure the VM image in cloud computing is comprehensive, with none of them adding more security requirements. Regarding overlaps between the security requirements and other approaches to securing the VM image, the majority of the experts did not identify overlaps between the provided security requirements. However, Expert G suggested that auditing could be substituted for accountability. Moreover, Expert D suggested that accountability is part of regulatory compliance, and so accountability can be removed.

7 Discussion

The experts reviewed the proposed framework in order to assess the importance of its factors. The majority of experts felt that the identified security requirements are important. A thematic analysis was used to examine themes within the interview results. According to the theme coding, the proposed framework factors are considered important when it comes to securing the VM image in cloud computing.

Expert B felt that regulatory compliance is not necessary to secure the VM image in cloud computing. However, regulatory compliance is one of the cloud control matrix components published by cloud security alliance [46], and for this reason regulatory compliance will be retained in the framework. Expert D argued that privacy is not important, although Mazhar et al. [18] identified privacy as an important requirement when it comes to securing the VM image in cloud computing. Therefore, privacy will also be retained in the framework. Similarly, although Expert D claimed that trust is ineffective in terms of securing the VM image in cloud computing, it is one of the cloud control matrix components published by cloud security alliance [46], and so trust is also retained in the framework. Regarding the overlap between the provided security requirements, there was no unified opinion among the experts in terms of whether there are overlaps between the proposed frameworks of the security requirements. Hence, none of the security requirements can be merged.

8 Conclusion and Future Work

As a brand-new processing paradigm, cloud computing leads to greater efficiency, minimised cost, and gives organisations round-the-clock access to a communal collection of resources and services; moreover, little is required in the way of management. In terms of elements which stand in the way of the adoption of cloud computing, security is one of the main hindrances; this is due to the fact that end-users' data are kept on the server(s) of the service provider. Discussion related to security issues has also taken into consideration the various cloud layers, with every layer accompanied by its own security problems. Of particular interest here is the virtualisation layer; indeed, the issues originating from this layer are among the most significant problems affecting the security of both the application layer and the data storage layer. As such, this study has put forth a framework focused on VM image security; the aim of this framework is to protect the VM image itself. Expert interviews were conducted in order to achieve the aims of this study; interviewees were experts in the field of cloud security. These interviews demonstrated that the theoretical security framework is sufficient to protect the VM image in cloud computing. Future work will involve questionnaires being distributed to cloud practitioners so as to further confirm the merits of the framework.

References

[1] R. K. Hussein, A. Alenezi, G. B. Wills, and R. J. Walters, "A Framework to Secure the Virtual Machine Image in Cloud Computing," 2016 IEEE Int. Conf. Smart Cloud, pp. 35–40, 2016.

[2] B. Hamlen, K., Kantarcioglu, M., Khan, L. and Thuraisingham, "Security Issues for Cloud Computing," Proc. - 9th Int. Conf. Comput. Intell. Secur. CIS 2013, pp. 150–162, 2012.

[3] M. a. AlZain, E. Pardede, B. Soh, and J. a. Thom, "Cloud computing security: From single to multi-clouds," Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 5490–5499, 2011.

[4] T. Swathi, K. Srikanth, and S. R. Reddy, "Virtualization in Cloud Computing," Int. J. Comput. Sci. Mob. Comput., vol. 35, no. 5, pp. 540–546, 2014.

[5] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[6] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[7] S. K. Abd, R. T. Salih, and F. Hashim, "Cloud Computing Security Risks with Authorization Access for Secure Multi-Tenancy Based on AAAS Protocol," IEEE Reg. 10 Conf. TENCON, pp. 1–5, 2015.

[8] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng. SOSE 2014, pp. 344–351, 2014.

[9] Q. Zhang, L. Cheng, and R. Boutaba, "Cloud computing: State-of-the-art and research challenges," Journal of Internet Services and Applications, 2010. [Online]. Available: http://download.springer.com/static/pdf/652/art%253A10.1007%252Fs13174-010-0007 6.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs13174-010-0007-6&token2=exp=1455281249~acl=%2Fstatic%2Fpdf%2F652%2Fart%25253A10.1007%25252Fs13174-010-000. [Accessed: 12-Feb-2016].

[10] B. P. Rimal, E. Choi, and I. Lumb, "A taxonomy and survey of cloud computing systems," NCM 2009 - 5th Int. Jt. Conf. INC, IMS, IDC, pp. 44–51, 2009.

[11] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," Telecomm. Policy, vol. 37, no. 4–5, pp. 372–386, 2013.

[12] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.

[13] F. Sabahi, "Virtualization-level security in cloud computing," in 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011, pp. 250–254.

[14] S. Carlin, "Cloud Computing Security," Artif. Intell., vol. 3, no. March, pp. 14–16, 2011.

[15] J. Recker, "Scientific Research in Information Systems," Springer Link, 2013.

[16] J. Kabbedijk, C.-P. Bezemer, S. Jansen, and A. Zaidman, "Defining multi-tenancy: A systematic mapping study on the academic and the industrial perspective," J. Syst. Softw., vol. 100, pp. 139–148, 2015.

[17] J. Espadas, A. Molina, G. Jim??nez, M. Molina, R. Ram??rez, and D. Concha, "A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures," Futur. Gener. Comput. Syst., vol. 29, no. 1, pp. 273–286, 2013.

[18] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci. (Ny)., vol. 305, pp. 357–383, 2015.

[19] F. Zhang and H. Chen, "Security-Preserving Live Migration of Virtual Machines in the Cloud," J. Netw. Syst. Manag., pp. 562–587, 2012.

[20] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," Proc. Annu. Hawaii Int. Conf. Syst. Sci., no. iv, p. 42, 2011.

[21] K. Sunil Rao and P. Santhi Thilagam, "Heuristics based server consolidation with residual resource defragmentation in cloud data centers," Futur. Gener. Comput. Syst., vol. 50, pp. 87–98, 2015.

[22] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW '09, no. Vm, p. 91, 2009.

[23] M. Kazim, R. Masood, and M. A. Shibli, "Securing the virtual machine images in Cloud computing," SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks, pp. 425–428, 2013.

[24] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, "Increasing virtual machine security in cloud environments," J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, p. 12, 2012.

[25] D. Jeswani, A. Verma, P. Jayachandran, and K. Bhattacharya, "ImageElves: Rapid and reliable system updates in the cloud," Proc. - Int. Conf. Distrib. Comput. Syst., no. i, pp. 390–399, 2013.

[26] K. Fan, D. Mao, Z. Lu, and J. Wu, "OPS: Offline patching scheme for the images management in a secure cloud environment," Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.

[27] A. Strauss and J. Corbin, "Basics of Qualitative Research," Basics of. Qualitatice Research 2nd edition. pp. 3–14, 1990.

[28] E. C. Crn, "Qualitative Research Methods," no. May, pp. 1–8, 2005.

[29] A. Bolderston, "Conducting a research interview," J. Med. Imaging Radiat. Sci., vol. 43, pp. 66–76, 2012.

[30] H. Sharp, Y. Rogers, and J. Preece, "Interaction design: beyond human-computer interaction," Book, vol. 11, p. 773, 2007.

[31] M. Saunders, P. Lewis, and A. Thornhill, Research methods for Business Students, Fifth edit. 2009.

[32] Arlene Fink, The Survey Handbook, 2nd editio. 2003.

[33] J. G. Geer, "What Do Open-Ended Questions Measure?," Public Opin. Q., vol. 52, no. 3, pp. 365–371, 1988.

[34] V. Lo Iacono, P. Symonds, and D. H. K. Brown, "Skype as a tool for qualitative research interviews," Sociol. Res. Online, vol. 21, no. 2, 2016.

[35] U. Reja, K. L. Manfreda, V. Hlebec, and V. Vehovar, "Open-ended vs. Close-ended Questions in Web Questionnaires," Dev. Appl. Stat., vol. 19, pp. 159–177, 2003.

[36] H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," Manag. Inf. Syst. Q., vol. 20, no. 2, pp. 167–196, 1996.

[37] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," Proc. - IEEE INFOCOM, 2010.

[38] V. Sekar and P. Maniatis, "Verifiable resource accounting for cloud computing services," Proc. 3rd ACM Work. Cloud Comput. Secur. Work., pp. 21–26, 2011.

[39] K. Popović and Z. Hocenski, "Cloud computing security issues and challenges," no. March, pp. 344–349, 2010.

[40] J. N. Ortiz, "Functional Encryption : Definitions and Challenges Introdu ¸ c ˜ ao," vol. 2, no. subaward 641, pp. 253–273, 2014.

[41] H. Chang and E. Choi, "User Authentication in Cloud Computing\nUbiquitous Computing and Multimedia Applications," vol. 151, pp. 338–342, 2011.

[42] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.

[43] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust," Acad. Manag. Rev., vol. 23, no. 3, pp. 393–404, 1998.

[44] R. Sandhu and S. Jajodia, "Integrity principles and mechanisms in database management systems," Comput. Secur., vol. 10, no. 5, pp. 413–427, 1991.

[45] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance & Security," 2013 Int. Conf. Availability, Reliab. Secur., pp. 546–555, 2013.

[46] Cloud Security Alliance, "Cloud Controls Matrix Working Group," 2014. [Online]. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/.