Solutions for Security Challenges in Cloud Computing – A Review

Rajesh Kalepu and C. Lakshmi Devasena
Department of Operations & IT, IBS Hyderabad, IFHE University, Hyderabad, India
devaradhe2007@gmail.com

Abstract*—*This literature review aims to identify the major security issues and their solutions in cloud computing security as well as identifying areas for future research. Utilizing a modified version of the approach suggested by Okoli and Schabram (2010) various articles were considered for the review. Although many security issues and solutions were identified in earlier research works, it is apparent that, much of the research being done based on considering only theoretical concepts of cloud computing. Thus this research review analyzed and explored plenty of issues that have been identified based on practical aspects of cloud computing, so that future research should focus more on the practical implications of these security risks.

Keywords—Cloud Computing; Security Issues; Cloud Security Risks; Cloud Security Challenges; Virtualization; Cloud service provider

INTRODUCTION

Cloud computing (CC) is a network model that makes it possible to attain on-demand network access and shared configuration resources, means that CC represents a framework for network access that doesn't need the same level of maintenance as a traditional organizational network would (Mell and Grance, 2011). Clouds are well integrated in our everyday life that most people don't even think about them being used. For example: iCloud, Office 365 and Google Drive. Since cloud computing is such a quickly expanding field within IT is not negligent to say that this network model has significantly changed how we observe networking today. In addition, it has also drastically changed how businesses, organizations and governments act and function. The growth of CC has brought with it new security challenges, which is why individuals and businesses alike act uncertain when confronted with the possibility of implementing a cloud solution (Subashini and Kavitha, 2011).

New security challenges leads to new opportunities for research, however this also means that an awesome amount of information available for organizations and individuals to goggle for information regarding CC security issues. Therefore this paper will present a literature review aiming to summarize the available information and make it more comprehensible.

1.1 Problem area

Initially it is important to mention that the reviewed subject (security issues and challenges) already has a solid foundation in the shape of pertinent literature. This review aims to analyze this foundation and summarize it in order to present the reader with an up-to-date, factual depiction of the present security risks and solutions within the CC field. The need for this is simple: since cloud computing endures to grow exponentially it is of absolute importance to stay updated on the current risks and solutions in order to ensure that future clouds are developed based on the cutting-edge insights. The problems presented in the massive amount of relevant literature have to sift through gain these aforementioned insights. Sometimes, it would be hard to know which literature is trustworthy in comparison with another. Thus, this review aims to analyze current literature within the CC field demarcated to security risks and solutions in order to form a concrete summarization which can then be used as an overview.

A summary produced in the form of Systematic Literature Review (SLR) would be of relevance to individuals and organizations, large and small, with a need for an up to date security overview as well as a tool for future research (Okoli and Schabram, 2010).

This literature review is built upon and discusses the following research questions:

1. What security risks and solutions are presented in the literature regarding cloud computing security?

2. What are the differences in security between public, hybrid, community and private clouds as well as the service models; IaaS, PaaS, SaaS and HaaS?.

The review is divided into five sections: introduction (1) definitions (2) Literature analysis (3) discussion (4) and conclusion (5).

DEFINITIONS

A. Security and information security

Information and communication technology (ICT) can arguably be considered a sub-component of information security since information security includes the protection of underlying resources. ISO/IEC 13335-1 (2004) defines ICT security as all aspects relating to defining, achieving and maintaining the confidentiality, availability, integrity, non-repudiation, authenticity, accountability and reliability of information resources. Thus, Solms and Niekerk (2011) argue that a clear understanding of these additional characteristics is essential as without them, information cannot be considered secure. As such, whenever this review utilizes the terms "security" or "information security", this is the definition being referred to.

B. Cloud Computing

Various cloud computing solutions exist, all with different types of characteristics. The different types of clouds are defined in this section, as well as the service models discussed in this review. Some key characteristics of CC are that it is capable of on-demand self-service as well as capable of rapid elasticity. This means that not only should a user be able to access the cloud without human interaction, in addition the cloud environment capabilities should be automatically scalable (Mell and Grance, 2011). It is important to know the difference between the different deployment methods as they can impact which security risks and solutions that are applicable to a cloud. The common ones are public, private, hybrid and community clouds.

1) *Public cloud*

The simplest way to describe a public cloud is an infrastructure that is used by the public and provided by a government, organization or other companies (Mell and Grance, 2011).

2) *Private cloud*

A private cloud is used exclusively by an organization and the cloud provider is either the organization themselves or a third party (Mell and Grance, 2011).

3) *Hybrid cloud*

A hybrid cloud is an infrastructure that combines public and private clouds. It consists of a composition of two or more clouds that all remain unique entities but are bound together by standardized or proprietary technology (Mell and Grance, 2011).

4) *Community cloud*

A community cloud is used by a community of consumers from various organizations that share common views. This particular setup may be controlled and maintained by a third party or by the organizations themselves.

C. Service models

Clouds use architectural models in order to provide different services to the users. Service models are not tied to a specific deployment type, public, private, hybrid and community, rather each deployment type can use each service model (Cloud Security Alliance, 2011). Just as with the different deployment methods the service models can have implications for a clouds security state, it is therefore important to have knowledge of these service models. The common service models are explained below.

1) *Infrastructure as a Service*

Infrastructure as a Service, often abbreviated to 'IaaS', consists of offering infrastructure solutions as a service. The major benefit of this is the ability to only pay for what you actually use. An example of this is Dropbox where the user can pay more or less depending on how much storage they need (Srinivasan et al., 2012).

2) *Software as a Service*

Software as a Service, often abbreviated to 'SaaS', utilises an instance of an application and the underlying database to offer the software to multiple customers simultaneously (Srinivasan et al., 2012).

3) *Platform as a Service*

Platform as a Service, often abbreviated to 'PaaS', provides a platform that can be used during the development of an information system, e.g. for testing and distribution. Examples of these kind of services are GAE and Microsoft Azure (Srinivasan et al., 2012).

4) *Hardware as a Service*

Hardware as a Service, often abbreviated to 'HaaS'. It brought forth a significant improvement because it allows for easy access to physical hardware devices, distributed among several geographical locations. If the cloud consumers subscribe to this service, it will appear as if they are connected to the local machine (Stanik et al., 2012).

D. Virtualization and multi tenancy

Virtualization and multi tenancy are two of the core technologies that enable CC to be used as we know it today. A traditional way of hosting applications and data storage involves running one operating system (OS) on one physical server. This traditional hosting method can also be used to create a functioning but inefficient cloud. This is achieved by linking multiple servers using a Virtual LAN (VLAN). This is secure but inefficient in the long term as a large part of the physical hardware available end up being unused. Virtualization was created in order to solve this efficiency problem. By using a Virtual Machine Monitor (VMM) a single physical server can host multiple instances of an OS. This means that a single server can utilize the available hardware power in a more efficient manner (Srinivasan et al., 2012).

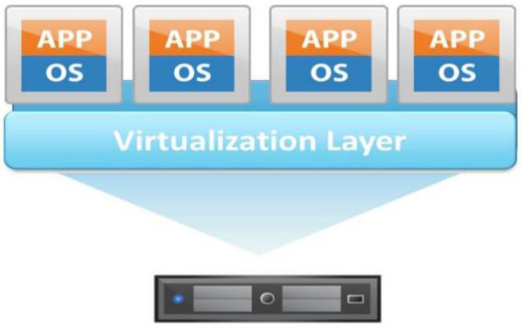

Fig 1. Descriptive image of Virtualization

Fig 1 is a basic illustration of a VMM running multiple instances of an OS using a virtualization layer. The virtualization layer is often known as hypervisor. There are two main ways of utilizing this hypervisor to run virtual machines (VM). These are known as full virtualization and para-virtualization. The difference between them lies in how much of the OS needs to be emulated. A VM deployed using full virtualization has to emulate the BIOS and drives of the OS, in addition to the other functions. A VM using para-virtualization

runs a version of the OS that has been modified to work without needing a BIOS or similar components (Mishra et al., 2013).

Multi tenancy is closely tied to virtualization. In short, multi tenancy allows several users to share computing resources with logical separation of the different users; a user in this case is a tenant of the system (Mishra et al., 2013).

LITERATURE ANALYSIS

In this section the security risks found in the literature as well as various solutions are presented. Solutions are discussed in the same section as their risks are discussed; however the solutionswhich are not specifically connected to a specific risk are discussed towards the end of this section.

A. Security risks

1) *Virtualization and multi tenancy*

While virtualization and multi tenancy are two staple technologies of CC they are still part of many security issues. The different types and different architectures for virtualization affect the security concerns related to these areas. However the difference between the different types of virtualization is less important than the overall cloud service type. It is also important to note that an emulated OS is still at risk from attacks that targets the traditional version of the OS. For instance a virtual machine running Windows is still at risk from attacks that target normal Windows machines. It is also important to note that hypervisors are additive to the overall security risk (Mishra et al., 2013)

As was just stated, normal security risks associated with operative systems still apply to virtual instances, however securing multiple virtual machines is more difficult. This stems from the fact that if one VM gets infected it can infect other VM since there is no need to bypass things such as network protocols; the infected VM is already inside the network. The infected VM can then perform VM to VM attacks or attacks against the hypervisor software (Mishra et al., 2013). Running antivirus software on the hosted VMs is all well and good but ensuring they are all up to date simultaneously is not so easy. If just one instance of the antivirus software is forgotten all VMs hosted on that platform are at risk. One solution to this is to run antivirus software on the underlying platform hosting the VMs. This antivirus would not be used to secure the platform itself, rather it would be used to monitor and secure all the data processed by the VMs. This means you only need to update one central antivirus in order to secure all the tenants on that physical server. Aside from this it also means that a virus attacking a VM will have a harder time affecting the overall antivirus system, since it resides outside the infected VM (Tari, 2014).

Another issue that might have a very severe negative impact on the organization using a cloud computing solution is data leakage. Data leakage occurs due to the shared resources used by the VMs. These can have the form of cache based attacks or RAM based attacks (Tari, 2014). These attacks occur since both the shared cache and RAM does not automatically flush upon completion of a computing task. This means a infected VM can recreate data based on the information left in the shared resources. In order to combat this hosting platform can inject ‘noise’ into the cache in order to flush if from any remaining information left behind by a VM (Tari, 2014). To combat the RAM based attacks it is necessary to restrict a VMs ability to lock the memory bus. Both of these solutions requires no expensive hardware modifications but can simply be introduced by adding software.

The risks associated with multi tenancy described above have slightly different implications depending on which service model is being used.

While the above mentioned solution with flushing the cache and preventing RAM bus locking works on all service models it is often better to prevent the issue from occurring in the first place. This is done by isolating the tenants from each other. In an IaaS environment this would mean isolating the data storage and processing resources. In a PaaS environment the isolation focus should be on isolating API calls as well as running services. In a SaaS environment the focus should instead be on isolating the transactions carried out on the same instance by different tenants. (Behl and Behl, 2012)

Regardless of the isolation degree chosen a user should never be fully aware of the exact server location for their data. While general information such as the country or region level is fine preventing the user from knowing the exact location decreases the risk of other malicious users learning the location. This means that multi tenancy attacks that rely on gaining access to a VM on the same physical server as the target will be much harder to achieve (Bouayad et al., 2012). For instance, a cache based attack cannot be used if the target VM is in another geographical location.

While isolation is a good solution it is important to note that it might mean less efficient resource sharing, this increases the cost and reduces the flexibility of cloud computing. An organization must therefore carefully consider the cost and benefit of increased isolation. While some data might be considered sensitive enough to warrant full isolation that is not necessarily the case for all the data used by the organization.

2) *Data privacy and integrity*

This ensures that the data is kept private and secure from unauthorized users as well as free from malicious or unintentional modifications is no easy task. When managing these aspects of security one main issue is the lack of control a cloud user has over the actual server the data is stored on (Chen and Zhao, 2012).

Data stored in the cloud can be divided into two groups, IaaS environment data and data in PaaS or SaaS environments. IaaS data is data that is stored in the cloud instead of on a local hard drive, examples of this include services such as Amazon Simple Storage Service. PaaS and SaaS data differs from this since this data is primarily used in applications processing the data, not necessarily storing it long term (Chen and Zhao, 2012).

Data stored in an IaaS environment can simply be encrypted in order to decrease the risk of private data becoming public. However this is not always as easy as it sounds as the encryption will only be as secure as the encryption method

chosen. Aside from this key management is a crucial issue (Behl and Behl, 2012). Often the users owning the data do not have the expertise needed to manage their encryption keys. Allowing the cloud service provider to manage the keys solves this problem but managing a large number of keys is a difficult task and the cloud service provider must have a secure way of doing this. Aside from this the entity responsible for key management must be a trusted entity. If the key management entity is not trusted by all parties the encryption might be rendered null and void seeing as there is no guarantee the keys will be kept out of reach from malicious interests. (Chen and Zhao, 2012)

For data used in PaaS or SaaS environments encryption is not a suitable solution. Seeing as the data has to be processed in an application it is not feasible to decrypt and encrypt the data for each computing task (Chen and Zhao, 2012). This means that data is left vulnerable to snooping co-tenants. While it has been shown that it is possible to perform some computing tasks on encrypted data it is not suitable for all types of computing (Tari, 2014).

Data integrity is a core part of managing data. Doing this in the cloud introduces new major challenges that must be solved if CC is to be considered secure. This is due to the fact that cloud servers are distrusted in terms of both security and reliability. The data stored in the cloud may be corrupted by both administrative errors as well as malicious attacks (Xiao and Xiao, 2014). Many cloud providers charge a fee for the uploading and downloading of data. This means that downloading large sections of data to verify the integrity of the data is not a viable solution. Some solutions have been proposed, including letting a trusted third party appointed by the cloud provider periodically check for data integrity. Despite this more research is needed to fully solve the data integrity issue. (Chen and Zhao, 2012)

Integrity is not only concerned with data. Software integrity also needs to be taken into account. Software integrity becomes a problem since the CSP provides the applications the user utilizes. Thus it is important that the software providers have a clear security policy on how to ensure that any software used will not do unexpected things to the users' data. (Zissis and Lekkas, 2012)

3) *Denial of service*

Denial of Service (DoS) or Distributed Denial of Service (DDoS) is one of the biggest security risks in cloud computing as well as any other internet based service. DoS or DDoS generally functions by the attacker sending large amounts of data packets, such as simple TCP/UDP or really any other type of data. The goal of a DoS attack is to negatively affect the availability of service for legitimate users by overloading the server's capacity and bandwidth (Rahman and Cheung, 2014 b). This is achieved when the host computer is unable to compute anymore data causing its many VM's to disrupt in their service, effectively making them unreachable by users (Rahman and Cheung, 2014 a).

DDoS is even more dangerous to cloud computing in comparison to other internet based services due to the nature of the attack. This is because DDoS takes advantage of hundreds of different computers, known as "bots", to attack a server using different types of data packets which makes it undeniably hard for a cloud service to defend itself. In addition to this, the VM configuration data is stored in the host computer. Thus, if an attacker gains access to the host he can simultaneously take control of all the VM's (Rahman and Cheung, 2014 a). DoS or DDoS attacks can take place against any type of cloud service such as IaaS, PaaS and SaaS as well as private, public, hybrid and community clouds (Rahman and Cheung, 2014 b).

A common solution to DDoS attacks is the use of a firewall (Liu et al., 2015). A centralized firewall has been proposed as a way to secure a cloud environment against a number of attacks. However such a centralized firewall comes with a number of disadvantages. Since a cloud environment runs many different services the number of rules the firewall will operate on as well as the package arrival rate allowed will be different for each service. In order to use a centralized firewall the rule set will grow to be far too large, and individual customers cannot specify separate rules for their cloud environment (Liu et al., 2015).

To solve this issue a decentralized firewall framework has been proposed. Such a framework has been shown to be cost effective (Liu et al., 2015). The framework operates by grouping multiple hosting servers into clusters; each cluster is then given dynamical resources to launch a VM instance that hosts the firewall for that specific cluster. This means that a customer can then rent a firewall for their specific application environment, allowing them to specify their own rule set and package arrival rate, thus solving the problem with a centralized firewall (Liu et al., 2015).

4) *Deduplication*

Deduplication is a technique where the server stores only a single copy of each file, regardless of how many clients requested the storage of the same file. By doing this the cloud servers as well as the network bandwidth are saved. However, deduplication may lead to leakage of sensitive side channel information. For instance a server utilizing this technology might get a request to store a file, however this file is already stored on the server. The server then tells the client making the request that the file already exists in the storage, and as such need not be transferred again. This would reveal to the client that another cloud user has the exact same file, which could be sensitive information in some cases. (Li et al., 2015).

B. Security solutions

1) *Security models*

Al-Anzi et al., (2014) suggest a security model for CC comprising governance, risk management and compliance. CC security requirements vary quite significantly from traditional environments because of its dynamic nature and customer ownership. It is pertinent to mention that this model can be applied to each type of cloud, e.g. private, public, hybrid and community as well as the different type of services; IaaS, PaaS and SaaS. Fig. 2 presents an overview of the security model and below it follows an elucidation.

Al-Anzi et al., (2014) suggest that an organization should implement a framework for effective risk management and measure the performance of the risk management by metrics.

People and identity management: Only authorized users should be able to access assets, an identity federation approach is applied in order to achieve secure authentication and authorization.

Application security: An XML signature as well as an XML encryption is implemented in order to protect applications from XML attacks and other web service attacks.

Information security: Data and information security is a top concern for any CSP as well as the customers using the service. As such, Al-Anzi et al., (2014) suggest that CSPs need to focus on how data is stored, processed and audited

Physical infrastructure: For physical measures they suggest the implementation of biometric access controls and a computer based access control system (CAS) which, in short, restricts access to users who can provide authorization.

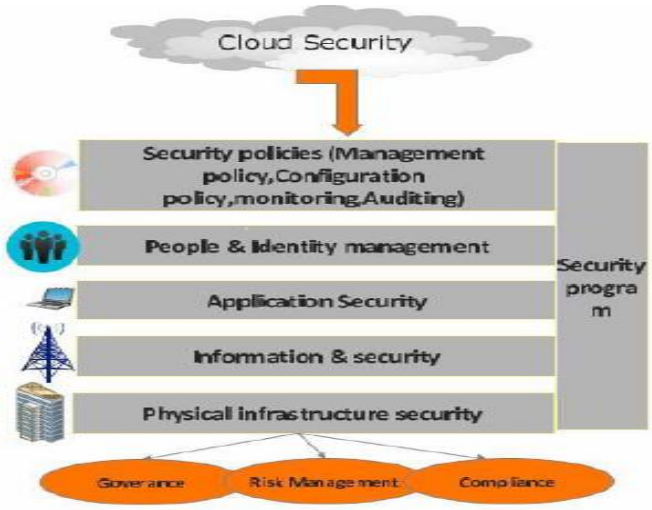

Figure 2. Security model (Source: Al-Anzi et al., 2014)

2) *Auditing*

Auditing within a CC environment basically refers to the process of ensuring data integrity of outsourced data and save the user's computation time and online burden of additional processing. Rewadkar and Ghatage (2014) propose a privacy-preserving third party auditing (TPA). TPA will verify the storage correctness of the outsourced data periodically when the users initiate a request for verification. The goal of the TPA is to reduce the burden of users by saving their computation resources while ensuring the correctness of their data stored in the cloud.

The problem that could arise by choosing not to use TPA is that CSP's, for monetary reasons, may delete data that is not being used or they may hide the data loss incidents to maintain reputation. Of course the users have the option of verifying this data themselves, albeit these options are impractical or risk the confidentiality of the data (Rewadkar and Ghatage, 2014). The solution will perform the auditing on the user's request. This will be done by sending the verification metadata from the user to the server and the response will then be verified by the TPA.

Another form of auditing is achieved by implementing a so called Trusted Third Party (TTP) which, in cryptography is an entity which facilitates secure interactions between two parties, e.g. a user and a CSP (Zissis and Lekkas, 2012).

3) *Policies*

Policies are often used as a way to ensure that organization wide security targets are being handled the same way across the organization. While policies on their own cannot solve security issues they are an important management tool. Cloud computing is no exception to this. When creating a policy regarding cloud computing it is important to remember that the cloud service provider must be aware of the policy. Indeed it might be wiser to develop a mutual understanding of the policy together with the service provider (Behl and Behl, 2012). This is also important due to the fact that the CSP might have several customers with different security needs and therefore it might be impossible for the CSP to create a policy that covers all the security needs of all the customers. Instead it is wiser to create policies that deal with individual customers and their specific needs (Sabahi, 2011). Ultimately a policy is only effective if the organization owning it continuously develops secure practices using the policy as a base.

4) *SecCloud*

SecCloud is a basic protocol which uses identity based cryptography. An overview of what this actually means and how it works is followed by the steps presented below, as described by Wei et al. (2014):

The System Initialization Operator (SIO) generates system parameters as well as master secret keys. After the system parameters are set the SIO selects a random number as its master key and another one for its public key. Once a user connects to the cloud it must first be registered with the SIO. The user can do this by using its unique ID, e.g. a user ID, and is then provided a secret key by the SIO through a TLS or SSL connection. Before the user can upload data to the cloud, the necessary storage for it is requested and is then allocated by the CSP. In an attempt to ensure data storage auditing, the user has to sign every single transmission block in order to generate authenticated data.

5) *Biometrics*

In many cryptographic systems the key to success lies on the client side, where cryptography and decrypting is stored. If this client in turn is attacked and hijacked by an aggressor, the whole cryptographic system is in critical condition. Rahman and Cheung (2014 b) have described ICMetrics technology as the possibility to produce unique identifiers based on the electric system's behavior which can then be used as a key. However, Tahir et al. (2013) argue that low entropy and a short key length for the ICMetrics key might make it sensitive to attacks. Thus, the authors suggest that this key has to be reinforced before it can be implemented as a security solution.

6) *Self-destructing data*

In order to combat the loss of control commonly associated with storing sensitive data in the cloud some researchers suggest implementing a self-destructing data scheme. At first glance this might seem like an odd solution. The idea is that self-destructing data gives the data owner control over their data even if they do not control the servers the data is stored on. By encrypting the data using a secure encryption method as well as a time span specified by the user the data owner can control how long the data will be available. The key used to decrypt the data is associated with the same time span as the encrypted data, and the key will only function as long as it is used within the given time span. After the times pan has expired the data can no longer be decrypted, and thus can be safely destroyed (Xiong et al., 2014).

Analysis and Discussion

During the process of analyzing the literature, the authors' of this review made a discovery. It appears as if literature that discussed a certain security topic often chose to focus on only one of the affected security areas. In the area of integrity the majority of the literature focused on data integrity whereas sub-areas such as software integrity and hardware integrity were basically non-existent.

This observation that the majority of the literature neglected sub-areas of their respective research could be considered a serious threat to the future of cloud computing. Another example is physical security. Physical is often mentioned in the literature; however it is seldom seen as a major security risk. Malicious or ignorant users are also often overlooked. While it is mentioned in a small part of the literature it is possible this particular risk is often overlooked due to how broad it is. Seeing as a malicious or ignorant user can be considered a threat in all areas of an organization it makes sense that it is not seen as a key threat in literature focused on a specific risk. The final example of this is the different service models and deployment models. Almost all of the literature included a definition for the different service models. Despite this only a small part of the analyzed literature attempted to distinguish unique security issues and solutions for each of the different service models. As the service models are a core part of cloud computing the authors' of this review consider this a major weakness in the available literature. The same can be said for the different deployment types; however the lack of discussion surrounding the different deployment types is not as severe of a flaw as it is in regards to the service models. This is due to the differences between the types of deployment being more obvious. For instance a public cloud is obviously more vulnerable to malicious users since the organization providing the cloud cannot maintain control over who use the cloud. Compare this to a private cloud where the cloud provider has a greater control over who gets access rights.

The lack of literature on these sub-areas can be explained in a few different ways. First, there is research conducted in these areas but it might not be published as a topic related to cloud computing security. For example the article related to HaaS written by Stanik et al. (2012) is published under cloud computing but not security nor cloud computing security. Second it might be possible that the sub-areas omitted from the majority of the research are not deemed important enough to warrant an entire paper. However it is most likely a combination of these reasons.

Conclusion

This review research could be concluded by answering the research questions.

What security risks and solutions are presented in the literature regarding cloud computing security?

It is clear that there is plenty of available research regarding cloud computing security. Even so, this review proves that it is still one of the predominant issues with the technology in its entirety. This review has managed to identified several significant security threats related to virtualization and multi tenancy, data privacy and integrity, denial of service, deduplication, user access control, loss of control, backup issues, availability, trust management and security in the different service models. The review also identified several different solutions to some security risks in the reviewed literature. The identified solutions were security models, auditing, policies, SecCloud, biometrics and self-destructing data.

What are the differences in security between public, hybrid, community and private clouds as well as the service models; IaaS, PaaS, SaaS and HaaS?

One important trend in the reviewed literature is the absence of research related to the differences in security between public, private, hybrid and community cloud deployment models. While a lot of the reviewed research included definitions for the different types of clouds merely a few of the twenty six journals and conference papers that passed the evaluation actually mentioned the security differences between a public, private, hybrid and community cloud. This is partially due to the fact that it seems many issues and solutions affect all four types. It is pertinent to mention that what was mentioned in this literature regarding security differences was miniscule at best. Thus, the conclusion was drawn to not present these differences in their own respective sections.

This review could serve as a theoretical basis for future research, showcasing the current major security issues as well as theoretical solutions. Future research should focus on practical case studies in order to validate the theoretical solutions discussed and presented in this review. Aside from this more research should be done in order to better understand the attitudes of cloud computing consumers as well as cloud service providers when it comes to security. Finally future research should strive to better understand the way the different deployment methods and service models affect the overall security of a system.

Acknowledgment

The authorsexpress their deep gratitude to the Management of IBS Hyderabad, IFHE University for the support and motivation extended.

REFERENCES

Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). *Cloud computing: Security model comprising governance, risk management and compliance*. In 2014 International Conference on Data Mining and Intelligent Computing (ICDMIC) (pp. 1–6).

Al-Anzi, F. S., Salman, A. A., Jacob, N. K., & Soni, J. (2014). *Towards robust, scalable and secure network storage in Cloud Computing.* In 2014 Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP) (pp. 51–55).

Behl, A., & Behl, K. (2012). *An analysis of cloud computing security issues.* In 2012 World Congress on Information and Communication Technologies (WICT) (pp. 109–114).

Bouayad, A., Blilat, A., El Houda Mejhed, N., & El Ghazi, M. (2012). *Cloud computing: Security challenges*. In Information Science and Technology (CIST), 2012 Colloquium in (pp. 26–31).

Chen, D., & Zhao, H. (2012). *Data Security and Privacy Protection Issues in Cloud Computing*. In 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 1, pp. 647–651).

Cloud Security Alliance. (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0.*

Li, J., Li, J., Xie, D., & Cai, Z. (2015). *Secure Auditing and Deduplicating Data in Cloud.* IEEE Transactions on Computers, PP(99), 1–1.

Liu, M., Dou, W., Yu, S., & Zhang, Z. (2015). *A Decentralized Cloud Firewall Framework with Resources Provisioning Cost Optimization*. IEEE Transactions on Parallel and Distributed Systems, 26(3), 621–631.

Mell, P., Grance, T. (2011). *The NIST definition of Cloud Computing*. (Artikelnr 800-145). National Institute of Standards and Technology.

Mishra, A., Mathur, R., Jain, S. & Singh Rathore, J. (2013). *Cloud Computing Security*. In International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC) (pp. 36-39).

Okoli, C., & Schabram, K. (2010). *A Guide to Conducting a Systematic Literature Review of Information Systems Research* (SSRN Scholarly Paper No. ID 1954824). Rochester, NY: Social Science Research Network.

Rahman, M., & Cheung, W. M. (2014) a. *Analysis of Cloud Computing Vulnerabilities.* International Journal of Innovation and Scientific Research, 2(2), 308–312.

Rahman, M., & Cheung, W. M. (2014) b. *Cloud Computing, Security Issues and Potential Solution by Using ICMetrics or Biometrics Based Encryption*. Intertional Journal of Advances in Computer Science and its Applications (IJCSIA) (Vol. 4: Issue 1. pp. 36-41).

Rewadkar, D. N., & Ghatage, S. Y. (2014). *Cloud storage system enabling secure privacy preserving third party audit.* In 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) (pp. 695–699).

Sabahi, F. (2011). *Cloud computing security threats and responses*. In 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN) (pp. 245–249).

Srinivasan, M. K., Sarukesi, K., Rodrigues, P., Manoj, M. S., & Revathy, P. (2012). *State-of-the-art Cloud Computing Security Taxonomies: A Classification of Security Challenges in the Present Cloud Computing Environment.* In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (pp. 470–476).

Stanik, A., Hovestadt, M., & Kao, O. (2012). *Hardware as a Service (HaaS): Physical and virtual hardware on demand.* In 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 149–154).

Subashini, S., & Kavitha, V. (2011). *A survey on security issues in service delivery models of cloud computing.* Journal of Network and Computer Applications, 34(1), 1–11.

Tahir, R., Hu, H., Gu, D., McDonald-Maier, K., & Howells, G. (2013). *Resilience against brute force and rainbow table attacks using strong ICMetrics session key pairs*. In 2013 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (pp. 1–6).

Tari, Z. (2014). *Security and Privacy in Cloud Computing.* IEEE Cloud Computing, 1(1), 54–57.

Von Solms, R., & van Niekerk, J. (2013). *From information security to cyber security.* Computers & Security, 38, 97–102.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). *Security and privacy for storage and computation in cloud computing.* Information Sciences, 258, 371–386.

Xiao, Z., & Xiao, Y. (2013). *Security and Privacy in Cloud Computing*. IEEE Communications Surveys Tutorials, 15(2), 843–859.

Xiong, J., Liu, X., Yao, Z., Ma, J., Li, Q., Geng, K., & Chen, P. S. (2014). *A Secure Data Self-Destructing Scheme in Cloud Computing.* IEEE Transactions on Cloud Computing, 2(4), 448–458.

Zissis, D., & Lekkas, D. (2012). *Addressing cloud computing security issues.* Future Generation Computer Systems, 28(3), 583–592.