Cloud Computing Security and Challenges: issues, threats, and solutions

Sadeem Hamad Alrasheed
Department of Information technology
College of Computer
Qassim University, Buraidah, KSA
431214114@qu.edu.sa

Majd Aied Alhariri
Department of Information technology
College of Computer
Qassim University, Buraidah, KSA
431114118@qu.edu.sa

Sulaiman Abdulaziz Aldubaykhi
Department of Information technology
College of Computer
Qassim University, Buraidah, KSA
431114111@qu.edu.sa

salim EL KHEDIRI
Department of Information technology
College of Computer
Qassim University, Buraidah, KSA
s.elkhediri@qu.edu.sa

Abstract— Cloud Computing has become of interest to everyone from institutions, companies, and individuals because of the many advantages it provides, and its low-cost infrastructure, in addition to the ease of managing it and accessing it remotely anywhere there is an Internet connection and it has become a great innovation in the information technology. With the rapid evolution of cloud computing, information security concerns have emerged that hinder the evolution of cloud computing and need a solution, as security has become the main challenge of cloud computing. This paper will focus on cloud computing security, challenges, issues, threats, and solutions.

Keywords— *cloud computing security, cloud computing management, cloud computing implementation, cybersecurity.*

1. Introduction

Cloud computing is not a new technology, the simple definition of Cloud computing is a sophisticated computing technology that allows to store, management, and sharing of data and software applications via a remote server and network from anywhere in the world online [1]. This term(cloud) means the use of the internet and remote server to derived from the commonest depiction in the network diagrams as an outline of a cloud, used to depict the transit of data from the cloud's carrier backbones to some endpoint location on the other side of the cloud it came in 1961 when the professor J.McCarthy suggested “that computer time-sharing technology might lead to a future where computing power and even specific applications might be sold through a utility-type business model” the idea of cloud computing became known in late 1960 [2].

Some Benefits of Cloud Computing, cost of cloud computing greatly succeeded in reducing costs for individuals and enterprises and indeed it proves this efficiency. Although it could be with unlimited storage, enterprises or individuals can have an unlimited capacity that can be used in the cloud. On the other hand, instead of storing data on a physical device, cloud computing can backup and recovery data at any time on any device. It uses an Automatic software integration that can automatically integrate and customize applications so that there is no need to do any efforts by the users, allows users to access information from anywhere that is connected to the Internet, as it solves the problems of time zone and geographical locations. Most importantly, it allows the benefit of quick deployment.

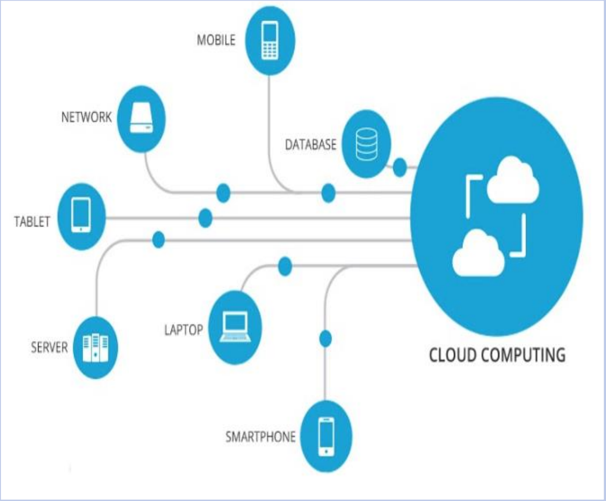

Figure 1. Cloud computing [2]

The system can run at full capacity in a few minutes, however, depending on the techniques used in the amount of time it takes. Figure 1, explains the uses of cloud computing.

2. REVIEW-RELATED SURVEY

In the last several years,, many survey papers have focused on security challenges in the cloud. In this article, we will provide a detailed look at security in the cloud. We will also cover challenges and issues in cloud security. Table 1 shows previous survey articles that focused on security challenges in the cloud.

In [3], Present all the potential security challenges in cloud computing and appropriate solutions to them in addition to proposing recent security frameworks to prevent potential attacks, also create security management for the cloud environment to reduce risks and increase trust in the cloud.

In this work [4], they presented the idea, characteristics, and architecture of cloud computing, in addition to urging companies and institutions to use cloud computing technology in business, on the other hand, they do not suggest using it in some sensitive applications such as banking services.

In [5], Discussing the challenges faced by security in vehicular cloud computing (VCC) and making a future guide to deal with them, in addition to discussing security attacks that harm the security of VCC and proposing solutions for them. Also, a detailed study on privacy issues in VCC security.

In this paper [6], the structure of the blockchain was discussed, in addition to discussing the characteristics of the

blockchain and cloud computing, proving the effectiveness of the blockchain technology in the cloud computing environment to provide high security in it, and presenting the current blockchain applications for cloud computing security.

In the last paper [7], it provides a thorough examination of the standards and procedures that govern data management and cybersecurity in cloud computing. in addition to addressing all forms of cybersecurity and special operations in cloud computing to achieve reliable and effective results, as well as managing cybersecurity controls to improve levels of security and confidence in the cloud computing environment.

Table 1. summary of the review-related survey.

Objective	Main Points	Year	Ref
Cloud Computing	- Analyzing the components of cloud computing and security and privacy problems. - Finding recent security solutions.	2020	[3]
Cloud Computing Security	- Provide an idea about the data and characteristics of cloud computing. - Presenting some problems and challenges of the cloud. - Suggesting the location of the cloud application.	2011	[4]
Cloud Computing in Vehicular	- Security problems of cloud computing for vehicles and their solutions. - Study of privacy and security of cloud computing for vehicles.	2020	[5]
Cloud Computing and Blockchain	-Discussing the characteristics of the blockchain and the cloud. -Proving the effectiveness of blockchain technology in cloud computing security.	2019	[6]
Cloud Computing and Cybersecurity	-Discussing Cloud Computing Concerns. -Establish policies that give a complete foundation for preventing cyber threats in cloud computing.. -Providing guidance to organizations on managing these risks.	2021	[7]

3. ARCHITECTURAL FRAMEWORK OF CLOUD COMPUTING

We can say that cloud computing combined several different technologies to give services to end-users. However, it is important to discuss the matter that contributes to cloud computing in order to comprehend risks of the security associated with cloud. Cloud computing definition in (NIST) [9], which is widely accepted [5]. NIST defines cloud computing as a three types service model figure(2). The fundamentals of cloud computing are explained below.

3.1 Essential characteristic of cloud computing

3.1.1. Broad Network Access

customers should be able to access cloud-based services, as well as their applications and data, by protocols and mechanism uses. Also requires that services be available to support a heterogeneous thin or thick environment such as(laptops, tablets, mobile phones, workstations). In the literature, ubiquitous accessing networks are frequently referred to as broad network access [10].

3.1.2 On demand Self service

Users are able to use the cloud to request and administer services from the cloud service providers (CSP) without third party between. They can access and get information and upgrade service whenever they need to. Use via Web services [10].

3.1.3. Resource Gathering

In a multi-tenant environment, the cloud's resources are shared by multiple clients . Clients are transparent about where the data are located. Clients are provided with a map for virtual and physical resources.

3.1.4. Measured Service

The use of services is measured and reported to the customer and cloud service providers, and the resources scaling up and down is done dynamically. Metering also assists in the automatic optimization of resource utilization, with users being charged on a pay-per-use basis.

The five characteristics of cloud computing that are above mentioned are defined by the NIST. On the other hand, The Cloud Security Alliance (CSA), defined multi-tenancy to be an essential characteristic as well [11].

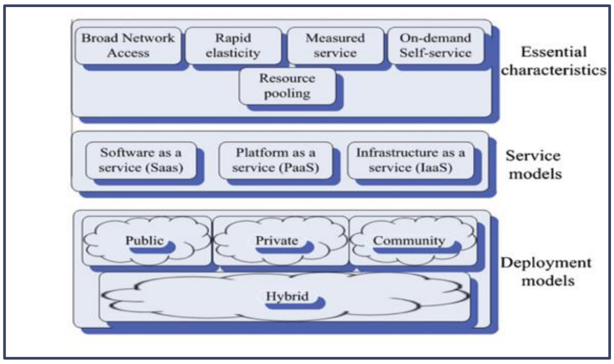

Figure 2. Cloud computing definition by NIST [13].

3.2 Cloud Service Models

There are three types of cloud services provided. Table 2 shows some examples

Table 2. Examples of Cloud service models.

Cloud service models	Examples
(SaaS)	Google Drive , Sales force, Go To Meeting, Dropbox, Amazon Web Services(AWZ).
(PaaS)	Windows Azure, Google App Engine, Apache Stratos, OpenShift.
(IaaS)	DigitalOcean, Linode, Rackspace, Cisco Metapod, Microsoft Azure.

3.2.1 Software As a Service (SaaS)

Customers can access CSP's apps, which are hosted on the cloud infrastructure, via the Internet using SaaS. Applications such as a web browser can be accessed using the thin clients interfaces. SaaS does not allow you to construct your own application or software. The SaaS model exclusively offers software via the Internet. Customers pay for consumption rather than ownership of the program [12].

3.2.2 Platform As a Service (PaaS)

Apps that are owned by customers need a framework to run and control. The aforementioned services are delivered via integrated development environments PaaS. Customers who use PaaS have no control over the underlying cloud infrastructure; instead, they have control over the programs that have been transferred to the cloud.

3.2.3. Infrastructure As a Service (IaaS)

IaaS refers to the physical infrastructure of a cloud service provider, that comprises network, storing, memories, processing, and other computing services. Virtualized systems that could be accessed through the Internet are used to make the resources available. The CSP has power over the underlying resources. [26]

3.3 Cloud Deployment Models

There are four different ways to set up a cloud computing infrastructure:

3.3.1. Public Cloud

The cloud's equipment is controlled and managed by the (CSP). The same resources are available to all clients. Customers pay the cloud owner according to the amount of time and resources they use. The hardware, which is located off-site from the clients, is operated by the CSP.

3.3.2. Private Cloud

Which is used and managed only by a specific organization. The organization may or may not own the physical infrastructure, and it may or may not be controlled by the organization or by a third party. Private clouds, on the other hand, may or may not be located at a company's actual location. A private cloud, in any event, is for the only use of a specific organization, with no other clients using the resources.

3.3.3. Community Cloud

Cloud that is shared by a group of organizations, consumers, or even both. The community's common interests include the goal, security measures, policy, and legal aspects. Any of the community's organizations, or a third party, could manage the community cloud. Similarly, it could be on/off site.

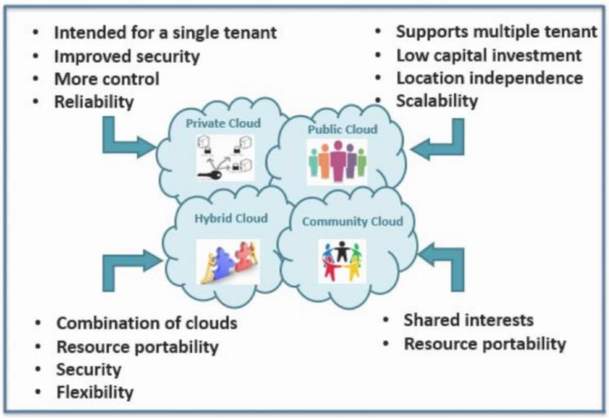

Figure 3. Attributes of cloud computing deployment models

4. CLOUD COMPUTING SECURITY CHALLENGE AND ISSUE

Cloud computing has added several of the useful services, it has raised a number of security problems and threats. Bad actors can take advantage of a number of weaknesses because a big amount of data is transmitted over the network and kept in specialized cloud resources. Figure 4 shows several concerns, which are explored in detail below.

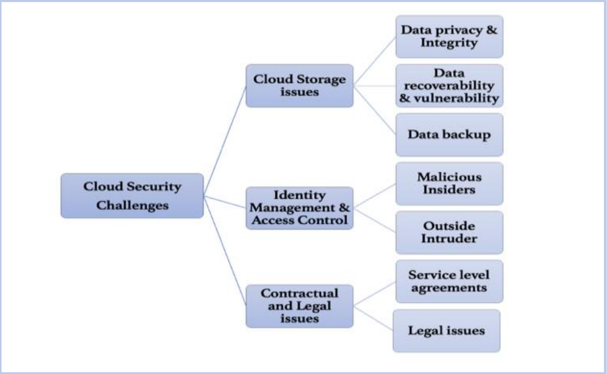

Figure 4. Cloud security Challenges [18].

4.1 Cloud Storage issues

Storing sensitive data with cloud storage providers poses significant security risks. The cloud can expose sensitive data, alter it, or return conflicting information to different users. Bugs, crashes, user errors, and misconfigurations are all possible [15]

4.1.1 Data privacy And Integrity

In order to implement security of user data stored in the cloud, each service provider must have a special policy and be fully aware of who has the right to access the stored data and that it cannot be maintained or modified in the cloud model; this can only be done by authorized persons. [16]. The security of cloud computing should be concerned with both the provider and the user. The user must preserve other users' data and not tamper with it, so the provider must provide a high level of protection for it. One of the most important benefits of cloud computing is saving money and additional storage of data, which can only be used if and only if both the provider and the user pay attention to security [17].

4.1.2 Data recoverability and vulnerability

Due to resource pooling and elasticity qualities in cloud computing, cloud provides customers with reactive and on-demand resource provisioning [18]. These characteristics may pose challenges in maintaining cloud computing security, such as unauthorized access management interfaces, intranet protocol weaknesses caused by wide network access, data retrieval due to Aggregation, and flexibility, which allows a user to recover data written by a previous user due to resource reallocation [19].

4.1.3 Data backup

When unintentional and/or purposeful disasters occur, data backup is crucial. To assure the data's availability, the Content Security Policy must execute regular backups. In reality, Backup data should follow security rules to prevent suspicious attacks such as modification and illegal access. [18].

4.2 Identity Management and Access Control

Access control and identity management are connected to the integrity and confidentiality of data and services. Keeping track of user identities is key to preventing unauthorized access to stored data. Because cloud computing's identification and access controls are complex, data owners and stored data are located on separate executive platforms [18].

4.2.1 Malicious Insiders

The worst event scenario for both cloud providers and cloud clients is a malevolent system administrator working for the cloud provider. Because of her business function with the cloud provider, the insider can use her authorized user credentials to examine sensitive data. For example, a system administrator in charge of performing frequent backups of the systems where client resources are hosted (virtual machines, data storage, etc.) could exploit her access to backups to exfiltrate sensitive customer data [20].

4.2.2 Outside Intruder

Outsider attacks are those that originate from a third-party source. Attacks are usually organized into incident groups. Many events are harmful in nature, while many others are not. For example, a person may mistakenly mistype a computer's address and connect to another system without permission [21]

4.3 Contractual and Legal issues

4.3.1 Service level Agreements

The Service Level Agreement (SLA) is a protocol that establishes a set of constraints and agreements between the user and the Cloud service provider. The following should be included in the SLA: Procedures done by the Content Security Policy in the event of a data breach, including remedial actions and a minimum performance level [18].

4.3.2 Legal Issues

The availability of Content Security Policy resources in geographically conflicting legal jurisdictions creates legal concerns. Different legal jurisdictions will cause an issue if the user is transferred from one geographic location to another [22].

4.4 Attack In Cloud Computing

In this part, we started an investigation into the challenges of cloud computing security. Now we want to highlight some of the attacks that face cloud computing and limit the application of security. Table 3 shows how we categories these attacks and problems linked to cloud computing security into five categories.

Table 3. Cloud Security category [28].

Category	Description
Security Standards	Interacts with regulatory and regulating agencies that create cloud security regulations in order to maintain a secure working environment in the cloud. Service level agreements, auditing, and other agreements between users, service providers, and other stakeholders are all included.
Network	Refers to the method by which users connect to cloud infrastructure in order to do computations. Browsers, network connections, and information exchange via registration are all part of it.
Access Control	Identification, authentication, and authorization issues fall under the Access Control category, which is a user-oriented topic.
Cloud Infrastructure	Security problems in SaaS, PaaS, and IaaS, as well as virtualization environments, fall under the Cloud Infrastructure category.
Data	Data such as data integrity and confidentiality

4.4.1 Theft of Service Attacks

Theft of Service attacks takes use of flaws in various hypervisors' schedulers. The attack is carried out when the hypervisor's routing protocol fails to identify and account for the CPU use of badly behaved virtual machines. This flaw could allow unscrupulous consumers to gain cloud services at the expense of others as a result of this failure [29].

4.4.2 Denial of Service Attacks

service (DoS) attacks. An attacker tries to make a system or network resource unavailable to its intended users in a DoS attack. One person or machine can launch a DoS attack. A real person or a group of zombies controlled by an attacker can be an attacker. With faked source IP addresses, an attacker can transmit enormous volumes of packets to the target [30].

4.4.3 Malware Injection Attacks

Injecting a malicious service implementation or virtual machine into the Cloud system is a first considered attack attempt. Such Cloud malware could be used for any purpose the attacker desires, by eavesdropping on data modifications to complete functional changes and blocking. To carry out this attack, the attacker needs create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS) and add it to the loud system. Also, the cloud system must be tricked into treating the new service implementation instance as a valid example of a service targeted by the attack. If this is effective, real user requests will be automatically sent to the malicious service implementation, which will run the adversary's malware. [31].

4.4.4 Attacks on Targeted Shared Memory

In this attack, attackers use shared memory caches or primary memory of both physical and virtual machines. It's a form of cloud computing attack that can lead to a variety of other attacks, such as side-channel attacks and malware injection attacks [32].

4.4.5 Phishing Attacks

In phishing attacks, the attacker manipulates a web link to redirect the user to a false link, allowing the attacker to obtain access to the information by hijacking the victim's account. Anti-spam software can be used to detect spam emails or pop-ups, as well as to protect against phishing assaults. [33].

4.4.6 Stepping-Stone Attack

The attackers attempt to accomplish their objectives (such as denial of service, and damage) also avoiding revealing their names and locations in order to reduce. This is accomplished by launching an indirect attack on the chosen victim via a series of other hosts (called stepping stones). Botnets that are illegal can be used to find stepping-stone hosts. the risk of discovery and trace-back. This is accomplished by attacking the chosen victim indirectly through a series of other hosts (called stepping stones). Illegal botnets can be used to recruit stepping-stone hosts [28].

4.4.7 Audio Steganography Attacks

Steganography is the use of common media files as a cover to transmit and hide confidential information. Therefore, the steganography technique is also used to leak data in cloud storage.

Where malicious insiders replace the less important parts of a media file with confidential information. The steganography media file does not look (sound) any different than the originals, with slight distortion in less prominent areas. As a result, in a cloud storage environment, the cover files should be freely exchanged. [34].

Table 1 Attacks against Clouds.

Attack Name	Effect	Category
Theft-of-service	· Using cloud services without being charged · Taking advantage of cloud resources at a low or free cost.	Cloud Infrastructure
Denial Of Service	· Inaccessibility of services/hardware · Putting a harmful code with an XML signature to obtain unauthorized access to information · Getting a hold of a browser's history or any other personal information	Network, Cloud Infrastructure
Cloud Malware Injection	· Leakage of confidential information · anomalous cloud machine behavior	Cloud Infrastructure
Targeted Shared Memory	· The data in the cloud resources leakage · User information/data leakage · Allows for new types of attacks, such as side channels and cloud malware insertion.	Cloud Infrastructure
Phishing	· Access to personal information without authorization · Putting dangerous software on a user's computer · Make the cloud computing structure behave erratically · Make the server inaccessible to the user.	Cloud Infrastructure, Network, Access
Stepping Stone Attack	· Unauthorized access to cloud resources · Make the cloud system work in an unusual way. Stealing sensitive information and Stealing user data.	Network, Cloud Infrastructure, Access
Audio Steganography	· Cloud storage system is unavailable · Accessing user data and User data deletion	Cloud infrastructure, Access

5. SOLUTION AND PRACTICES FOR CLOUD SECURITY CHALLENGES

Because more people are realizing the benefits of cloud computing, it is becoming more popular. It allows the user to simply reduce the size of the operation while also saving money. However, as the use of cloud services has grown, so have

security concerns and risks [23]. There are some technologies and practices that can helps to increase storage capacity in addition to storing information securely

5.1 Vulnerability Shielding

Through the cloud service provider, patch management must be improved. They should check the vulnerability of their cloud service on a regular basis and always update and maintain it to minimize the number of possible access points and reduce the chance of a hacker attack on the cloud. The service provider must deploy an Intrusion Detection System (IDS) to ensure that the cloud service is safe and secure [24].

5.2 Service Provider Properties

Each service provider has its own data management methods, so be sure to look for a suitable cloud service provider eg one that is experienced and trustworthy [25].

5.3 Security check

One of the most important guarantees for cloud services is to establish a contract with the service provider so that users can claim claims in the event of data breaches or mishaps [24].

5.4 Access control

Users authorized to access data through the cloud service provider must be validated at any time, as the data access control is set up by the service providers. The service provider must also set the authorized users to access the data stored in the cloud. The strategy can help to lower the danger of unauthorized people accessing data and to provide a secure storage space to store important data [24].

6. ORGANIZATION

Some organizations are seeking to make the shift to cloud computing easier. NIST and ENISA are governing bodies in the United States and the European Union. Consortia of representatives from industry research and design, suppliers, vendors, customers, academia, and, in certain circumstances can be government.

6.1 National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) aims at the network and information security. NIST investigates information security to address and prevent security issues. NIST coordinates the development and exchange of best practices and advice among businesses, industry, institutions. NIST houses the Information Technology Laboratory that directs the nation and federal agencies on aspects connected to information systems and security.

6.2 European Network & Information Security Agency (ENISA)

As stated previously, the European Network & Information Security Agency (ENISA) is much similar in nature to NIST but it's an agency of the European governments.

6.3 Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) has a strong presence in the cloud risk and security field. The CSA was formed in April 2009 and is composed of information security researchers and professionals from the biggest company that specialized in computing and information technology like RSA Security, Barclays, and Qualys. CSA members are (47%) from North America, (34%) from Europe, and the rest are from Africa, Middle East and Asia. they interesting on the aspect of security assurance in cloud computing

6.4 Open Group (OG)

The global consortium that uses technology standards to help businesses achieve their goals. Customers, systems and solution providers, tool vendors, integrators, academics, and consultants from a variety of industries make up our diversified membership of over 800 organizations.

7. CONCLUSION

Cloud computing uses spread widely into our communities more than ever. People must learn and read about cloud computing, security, challenges, attacks, solutions, and history to cover most weaknesses of awareness and help them to reduce financial and data losses. A lot of companies are facing a difficult situation to choose cloud services or using inappropriate services. But knowing the services provided and their uses, advantages, and weaknesses could help them to solve these problems. This paper presented a general history of cloud computing and a review of some previous papers in cloud computing, the architectural framework of cloud computing and security challenges to develop solutions to them were also presented, and finally the organizations that research and develop in the cloud computing security were discussed.

REFERENCES

[1] Mell, P., & Grance, T. (2009, 7 10). The NIST Definition of Cloud Computing, from NIST Information Technology Laboratory, retrieved on April 2011.

[2] Rittinghouse, J., & Ransome, J. (2009). Cloud Computing: Implementation, Management, and Security (1st ed.). CRC Press.

[3] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A Survey On Security Challenges In Cloud Computing: Issues, Threats, And Solutions". The Journal Of Supercomputing, vol 76, no. 12, 2020, pp. 9493-9532. Springer Science And Business Media LLC, doi:10.1007/s11227-020-03213-1.

[4] Arockiam, L., S. Monikandan, and G. Parthasarathy. "Cloud computing: a survey." International Journal of Internet Computing 1.2 (2011): 26-33.

[5] Goumidi, Hadjer, Zibouda Aliouat, and Saad Harous. "Vehicular cloud computing security: A survey." Arabian Journal for Science and Engineering 45.4 (2020): 2473-2499.

[6] Gupta, Ashok, et al. "Cloud computing security using blockchain." Journal of Emerging Technologies and Innovative Research (JETIR) 6.6 (2019): 791-794.

[7] Tissir, Najat, Said El Kafhali, and Noureddine Aboutabit. "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal." Journal of Reliable Intelligent Environments 7.2 (2021): 69-84.

[8] Priya Viswanathan, Cloud Computing - Is it Really All That Beneficial? Advantages and Disadvantages of cloud computing.

[9] P. Mell, T. Grance, The NIST definition of cloud computing (draft), NIST Special Publ. 800 (145) (2011) 7.

[10] D. AB. Fernandes, L. FB. Soares, J.V. Gomes, M.M. Freire, P. RM Inácio, Security issues in cloud environments: a survey, Int. J. Inform. Sec. 13 (2) (2014) 113

[11] Cloud security alliance, security guidelines for critical areas of focus in cloud computing v3.0, 2019.

[12] L. FB Soares, D. AB Fernandes, J.V. Gomes, M.M. Freire, P. RM Inácio, Cloud security: state of the art, in: Security, Privacy and Trust in Cloud Systems, Springer, Berlin, Heidelberg, 2014, pp. 3–44.

[13]ENISA, 2009b. Cloud computing benefits, risks andrecommendations for information security. November, 2009.

[14] An Overview of Cloud Computing - Universal Web Server. (2021). Retrieved 3 December 2021, from https://universalwebserver.com/an-overview-of-cloud-computing/

[15] Popa, R. A., Lorch, J. R., Molnar, D., Wang, H. J., & Zhuang, L. (2011, June). Enabling Security in Cloud Storage SLAs with CloudProof. In USENIX Annual Technical Conference (Vol. 242, pp. 355-368).

[16] Hamlen K, Kantarcioglu M, Khan L and Thuraisingham B 2012 Security issues for cloud computing Optimizing Information Security and Advancing Privacy Assurance: New Technologies 8 150-162

[17] Jain S, Kumar R, Kumawat S and Jangir S K 2014 An analysis of security and privacy issues, Challenges with possible solution in cloud computing Proc. of the National Conf. on Computational and Mathematical Sciences (COMPUTATIA-IV) 1-7

[18] Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135.

[19] Youssef, A. E., & Alageel, M. (2012). A framework for secure cloud computing. International Journal of Computer Science Issues (IJCSI), 9(4), 487.

[20] Kandias, M., Virvilis, N., & Gritzalis, D. (2011, September). The insider threat in cloud computing. In International Workshop on Critical Information Infrastructures Security (pp. 93-103). Springer, Berlin, Heidelberg.

[21] Patel, Ahmed, et al. "An intrusion detection and prevention system in cloud computing: A systematic review." Journal of Network and Computer Applications 36.1 (2013): 25-41.

[22] B. Hay, K. Nance, M. Bishop, Storm clouds rising: security challenges for IaaS cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.

[23] Mell P and Grance T 2011 The NIST definition of cloud computing Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-145

[24] Y.Z.An, Z.F.Zaaba and N.F.Samsudin, Reviews on Security Issues and Challenges in Cloud Computing, IOP Conference Series: Materials Science and Engineering, 160 (1) (2016).

[25] Ramanathan S, Goel S and Alagumalai S 2011 Comparison of cloud database: Amazon’s SimpleDB and Google’s Bigtable International Journal of Computer Science Issues 8 6 2.

[26] K. Hashizume, D.G. Rosado, E.Fernndez-Medina, E.B.Fernandez, An analysis of security issues for cloud computing, J. Internet Services Appl. 4 (1) (2013) 1–13.

[27] Khalil, A. Khreishah, and M. Azeem, “Cloud Computing Security: A Survey,” Computers, vol. 3, no. 1, pp. 1–35, Feb. 2014.

[28] Fangfei, Z.; Goel, M.; Desnoyers, P.; Sundaram, R. Scheduler vulnerabilities and coordinated attacks in cloud computing. In Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 25–27 August 2011;

[29] Yan, Q., & Yu, F. R. (2015). Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 53(4), 52-59.

[30] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE international conference on cloud computing (pp. 109-116). Ieee.

[31] Khorshed, M.T.; Ali, A.B.M.S.; Wasimi, S.A. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Gener. Comput. Syst.

[32] Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[33] Amara, N., Zhiqui, H., & Ali, A. (2017, October). Cloud computing security threats and attacks with their mitigation techniques. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 244-251). IEEE.

[34]Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B., & Su, J. (2011, December). Thwarting audio steganography attacks in cloud storage systems. In 2011 International Conference on Cloud and Service Computing (pp. 259-265). IEEE.