A Survey on the Security of Cloud Computing

Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri, Noof Alarifi

Computer Sciences Department

College of computer science & information Sciences

King Saud University

Riyadh, Saudi Arabia

***Abstract*—Within the recent decade, major innovations in technology have emerged, that potentially add more convenience to daily life practices not only on an enterprise level but on an individual level as well. Cloud Computing technology has witnessed significant advances in its implementation and become widely adopted by either private or public sectors. It was obvious recently that a lot of organizations and enterprises are transferring their workloads to the cloud. However, security is a major concern for the cloud computing services which is based on Internet connection that makes it vulnerable to multiple types of attacks. Even though that the security measures implemented over cloud computing are developing every passing year, Security still a challenge. In this paper, we conducted a survey study on cloud computing and addressed different types of attacks and possible threats to this emerging technology, as well as protection methods and existing solutions to such attacks.**

Keywords— Cloud Computing; Information Security; Cyber-attacks; Threats.

I. Introduction

Cloud computing (CC) technology has been broadly utilized in many areas, including file sharing, real-time applications, and communication. Major CC innovations have emerged within recent decades, including significant advances. CC has become widely adopted in both the private and public sectors due to the practicality of its services, which can potentially add convenience at several levels. On the other hand, the security of the provided services is a primary concern for both cloud users and cloud service providers [1].

Cloud Computing security is an essential subdomain of computer security, and it poses a major challenge to cloud technologies' widespread adoption. Because CC services are essentially based on an Internet connection, they are vulnerable to a variety of attacks and other security threats, which can result in potentially severe impacts such as data breaches, malware injections, denial-of-service (DoS) attacks, data losses, and insecure application programming interfaces (APIs) .According to [2], security incidents in the cloud environment have grown notably over the few past years probably due to the remarkable growth in cloud services [3].

For this paper, we conducted a survey on Cloud Computing to address various types of attacks and other threats to this progressing technology, as well as potential protection methods and the existing solutions to such problems.

The remainder of this paper is structured as follows. Section II presents an overview of CC, including its architecture, deployment models, and advantages and disadvantages. In Section III, we discuss the CC security models, requirements, and policies, followed by an intensive study of CC security threats and the possible solutions to the existing problems in CC. Section IV comprises the conclusion.

II. Overview on Cloud Computing

Cloud Computing is defined by National Institute of Standards and Technology (NIST) as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

This section provides a brief overview of CC technology, including its architecture, service models, deployment models, and advantages and disadvantages. The essential CC characteristics are illustrated in the following subsection.

A. Architecture of Cloud Computing

The cloud architecture is generally classified into three cloud-service models: infrastructure-as-a-service (IaaS), the lowest layer, which provides fundamental infrastructure for the other layers; platform-as-a-service (PaaS), the middle layer, which provides an environment for developing and hosting users' applications; and software-as-a-service (SaaS), the upper layer, which provides an application layer that works as a service on demand. This architecture follows a bottom-up approach [4],[5] as shown in Fig 1.

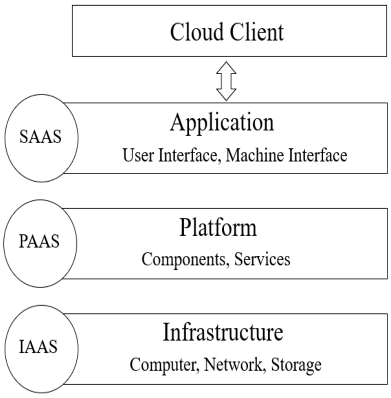

Figure 1: Service Model in Cloud Architecture

978-1-7281-0108-8/19/$31.00 ©2019 IEEE

1) Software-as-a-Service (SaaS)

SaaS is also known as on-demand service that allows customers to utilize applications that are hosted on a cloud server and delivered over the Internet; this can include online office suites and e-mail applications. Users can subscribe to web-based software services to handle their business's needs at a small cost instead of purchasing new software. The consumers depend on the providers for security. SaaS does not require the users to have special hardware of a software; however, it does require a permanent Internet connection [6], [7].

2) Platform-as-a-service (PaaS)

PaaS, the layer beneath SaaS, allows developers to efficiently write and develop SaaS applications and deploy them on the PaaS layer. PaaS completely supports the software life cycle, and it is an economical option for developers, as it allows them to concentrate on building and running applications rather than on monitoring the underlying infrastructure. The service providers are responsible for constructing and maintaining the infrastructure for the developers [6].

3) Infrastructure-as-a-service (IaaS)

IaaS, the lowest layer, provides the fundamental infrastructure for the above layers. IaaS includes networking hardware, servers, operating systems (OS), and storage. It allows consumers to utilize complete resources without purchasing physical equipment. IaaS is also cost-effective and faster choice for operating the workload without the need to purchase or manage the underlying infrastructure; however, as it is based on Internet connectivity, availability is a primary concern [7],[8].

B. Deployment Model of Cloud Computing

There are four main deployment models for Cloud Computing proposed by NIST [1], public clouds, private clouds, hybrids clouds, and community clouds.

1) Public Cloud

In a public cloud environment, hardware and software resources are publicly shared among different users. A third-party public-cloud service provider manages and monitors this environment, so such clouds are suitable for information that is not sensitive [3], [9].

2) Private Cloud

A private cloud is operated by a single organization; all of a given cloud's systems and services are only accessible within the boundaries of that organization. The company handles all the management and maintenance related to the infrastructure; a private cloud is thus very expensive, but it is more secure than a public cloud [6], [9].

3) Hybrid Cloud

A hybrid cloud is a combination of two or more types of clouds (e.g., a public–private cloud). Because it exhibits the features of the involved clouds, this type of deployment model provides high scalability and flexibility, as well as many options for data deployment. A hybrid cloud is managed centrally [6], [9].

4) Community Cloud

Community clouds are similar to public clouds in many aspects; however, this cloud-service model is usually intended for specific individuals, businesses, or organizations that share the same cloud requirements. In a community cloud, either participating community members or a third-party service provider can manage the shared resources [3],[6].

III. Security in Cloud Computing

A. Cloud Computing Security Requirements

Confidentiality requires blocking unauthorized exposure of CC service users' information. Cloud providers charge users to guarantee confidentiality; in CC, the focus is on authentication of cloud resources (e.g., requiring a username and password for each user). Moreover, Availability is the ability for the consumer to utilize the system as expected. A client's availability may be ensured as one of the terms of a contract; to guarantee availability, a provider may secure huge capacity and excellent architecture. Accountability involves verifying the clients' various activities in the data clouds. Accountability is achieved by verifying the information that each client supplies (and that is logged in various places in information clouds).

B. Classification of Cloud Security Issues

CC contains many categories, each of which has many security concerns. The security issues occur throughout CC hardware, software, and communication. Data defects in cryptographic methods can cause security issues in data centers or in communication. These issues can also come from the customer if the authentication policy is weak.

1) Embedded Security

Embedded systems have the advantages of high-quality tools and require the user to connect to a local network to unlock the debug ability. The main CC security issues in the embedded system are due to the use of VMs [10]. Such systems have the advantages of strength and isolation. However, a VM can have a real security threat when a problem with deployment occurs. Data leakage can arise through the implementation of separate VM workloads. Thus, CC providers should be careful when uploading isolated VMs into the infrastructure. In addition, in VM monitoring, the host computer works as a controlling point, as the host machine can update and change any resources in the VM [11].

2) Application

The most sensitive and vulnerable areas of any system are software applications. Software includes both a front end and a back end on many platforms and frameworks. The huge amount of software code [12] is the primary cause of security concerns. When an application has many programmers and/or coding languages, many vulnerabilities can arise [13].

3) *Client Management*

Clint management is a security matter in the CC environment. Client management simply involves protecting the public information in the client's system. The client's experience plays an important role in a cloud, as cloud services are growing so fast that the industry is experiencing an overall service increase. That's why some providers are struggling due to the deployment of weak solutions to the user. Some users with experience in the cloud security field will struggle when choosing a cloud provider. User authentication plays a great role in protecting the cloud from strictly illegal access [14],[15].

4) *Cloud Data Storage*

The most significant component of CC is cloud data storage. Given the current growth in online applications and the connected devices, the security issues related to cloud data storage are becoming more important. Data warehouse deployment requires high security, which reflects the quality of the cloud service [16].

5) *Cluster Computing*

A computer cluster involves multiple computers, VMs, or servers that are connected together to run as a single system. Industrial CC uses the idea of clustering for parallel processing. This technique has many advantages, but it can cause security challenges due to the increase in users in each cluster [17].

6) *Operating System Based*

Many security issues can arise within a CC system that uses many VMs, many servers in different networks, or multiple operating systems. Desktop operating-system virtualization separates the physical client from the desktop environment. Remote desktop virtualization is used in clouds to offer clients access to servers' computing power. Server operating-system virtualization can be used for remote code execution. Network operating-system virtualization involves the use of routers and firewalls for a specific user. The security issues for such services include the limitations of the default installation settings and the potential for unpatched security systems on the machines. Smartphones' operating systems have access to cloud services, which can exponentially increase the availability of applications. As the number of smartphones increase, so does the rate of malware development. Attackers are gaining interest in attacking smartphone operating systems. Related security issues include client-side injection and destroyed cryptography.

IV. Threats and Countermeasures in a Cloud Computing Environment

A threat is a possible cause of an incident; it may result in harm to a system or an organization. This section provides specifications on the most dangerous threats in CC. Each threat is described in detail and some suggested solutions are also given.

A. *Data Loss*

Data losses can occur for various reasons, both intentional and unintentional; actions with both good and harmful intentions can lead to data losses. Data can be lost due accidental deletion or alteration. Additionally, for encrypted data, the loss of the encryption key can cause data loss. Natural causes (e.g., earthquakes or fires) are also possible. In CC, the threat of data loss affects IaaS, PaaS, and SaaS cloud services. CC providers should cover the data-loss aspect to ensure reliability, usability, and extensibility. Even though the cloud provides cost-saving methods, these methods should not compromise the users' data [18].

Institutions use CC to store data, and they expect to receive the promised levels of data integrity and safety. However, as the cloud is a multi-tenant environment with various authorities and access methods, unauthorized users need to be detected and prevented from accessing data and services. Although this is not an easy task, it needs to be correctly addressed and managed. Data loss can cause financial losses for customers and reputation losses for institutions. Specifically, incomplete authentication, authorization, or accounting controls; undependable encryption algorithms or keys; operational failures; political matters; and data-center reliability are the main causes of direct and indirect data loss [19],[20].

B. *Data Breaches*

Data breaches involve the release of critical information to unauthorized parties, such that malicious people gain access to a network and its sensitive data. A data breach can occur due to many causes, including incorrect authentication or authorization mechanisms, poor review of controls, undependable use of encryption keys, and operating-system failures. Apple (iCloud), Microsoft, Yahoo, and Google are some of the organizations that have faced this threat. In CC, the data-breach threat affects IaaS, PaaS, and SaaS cloud services.

Unfortunately, although data leakage is a critical threat in CC, the solutions and mitigating action can cause other threats to arise. Encrypting the data can reduce the effect of a data breach, but it can also lead to data losses when the encryption keys are lost [21],[22].

C. *Insecure Interfaces and Application Programming Interfaces*

Cloud users utilize APIs to communicate properly with cloud services. Cloud providers usually publish a number of APIs that permit users to develop their own interfaces for communication. The types of communication that APIs offer include supply, management, concurrency, and monitoring of the cloud processes. The security and availability of the cloud services are reliant on the security of these APIs. From the early stages of authentication and access control to the encryption and monitoring processes, these interfaces need to be designed to defend against both unintentional and malicious attempts to attack [23].

However, these interfaces increase the complexity of a cloud by adding a layer on top of the framework. This allows the API's weaknesses to spread in the cloud environment.

Moreover, institutions may be required to give their credentials to third parties in order to enable their services specified by the developed APIs. In CC, the insecure interface and API threat affects the IaaS, PaaS, and SaaS cloud services [21],[20].

D. *Malicious Insiders*

The malicious-insider threat arises from trusted people within the cloud organization who have authorized access to the organization's assets and items of value. These people can apply unprivileged operations to cause harm to the organization's assets. The harm can be financial loss, technical failure, or resource loss and can occur due to what seem to be legal activities (e.g., developing malicious firewalls) [24]. This threat is critical to address because insiders are harder to detect than outsiders. Giving authority to employees is the main concern here because they are the gateway to this threat. In CC, the malicious-insider threat affects IaaS, PaaS, and SaaS cloud services [25].

Insider attacks are launched by malicious employees at the provider's or user's site. It is a well-known fact that most security threats arise from the inside of an organization. A malicious insider can easily gain passwords, encryption keys, and data [26],[27].

E. *Account, service and traffic hijacking*

Account or service hijacking happens if an attacker gains the login information of an account, which makes the hacked account a launching base for the attacker. By acquiring the account credentials, the attacker can snoop on customer businesses, refund wrong information, manipulate data, and redirect the customer to other places to perform additional attacks. In cloud-account hijacking, a malicious intruder can use the stolen credentials to hijack the cloud services and then enter into others' transactions, add incorrect information, and divert users to illegal websites, causing legal issues for cloud service providers. This threat is widespread and critical nowadays; many attackers obtain the account credentials of various cloud consumers [22].

These kinds of attacks involve the ability to obtain stolen credentials. There are different attack approaches for stealing credentials, such as phishing, fraud, DoS, and finding vulnerabilities. In CC, the account, service, and traffic hijacking threat affects the IaaS, PaaS and SaaS cloud services [28].

In this section, we sought to mention and summarize the most effective threats in CC. Mitigating these threats is essential to cloud providers and users. However, the priority given to some of these threats over others depends on the cloud application and usage. Concluding our discussion of this matter, the challenges of developing solutions to each threat will be listed. These challenges have to be studied and addressed in order to overcome the cloud threats. Table I lists the threats and the challenges associated with their remediation development. These challenges can arise from the cloud providers, users, environment, and many other sources.

TABLE I. CHALLENGES TO THREAT REMEDIATION

Threat	Challenges
Data Losses and Breaches	• Trust issue with the cloud providers. • Untested procedures, standards, and insufficient data preservation methods. • Absence of knowledge.
Insecure Interfaces and APIs	• Incapability of reviewing events associated with API use. • The APIs' complexity.
Malicious Insiders	• Providers hide their company strategies from employees. • Lateness of solutions developed after the incident occurs. • Incapability of cloud providers to monitor employees.
Account, Service, and Traffic Hijacking	• Fast growth of CC opens new gaps. • Current method of digital identity management is not good enough for hybrid clouds.
Shared-Technology Vulnerabilities	• Development of shared components is not guaranteed. • The use of VM technology. • Mapping between the manufacturing process and allotment process of shared components.
Abuse of Cloud Services	• Cloud providers' limited ability to monitor due to privacy laws. • Stakeholders' varied interests.

V. ATTACKS AND COUNTERMEASURES IN A CLOUD COMPUTING ENVIRONMENT

The key motivation of this research is to determine the potential attacks in the CC environment and their possible solutions. CC offers services using IaaS, PaaS, and SaaS, as shown in Figure 1 [29]. In this paper, we classified the attacks based on the service delivery model of CC [30]. By exploiting vulnerabilities in the cloud, as explained in Section IV, an adversary can launch various attacks. The following subsections outline the key attacks under each category.

A. *Security attacks on SaaS cloud layer*

In SaaS, most users are still uncomfortable with the SaaS model due to data-related security issues such as who owns the data, data backup, data access, data locality, data availability, identity management, and authentication [31]. We consider famous types of security attacks on the SaaS cloud layer, as elaborated below.

1) Denial of service (DoS) attacks

DoS attacks are the most prominent attacks in the CC environment. The main aim of the attacker is to exhaust all the resources of the victim by sending thousands of request packets to the victim over the Internet. In fact, the rate of DoS attacks is increasing due to some characteristics of CC, such as on-demand services, self-service, and broad network access. DoS attacks target the availability of the services provided by the cloud in order to flood a network. Thus, they reduce the user's bandwidth, disrupt service to a specific system, and prevent the user from accessing or using the cloud service. There are many types of DoS attacks, such as Distributed DoS

(DDoS) attacks, which are extended from DoS attacks and involve the attacker using numerous network hosts to inflict more devastating effects on the victim [32],[33].

2) Authentication attack

The identity is used to identify users to achieve secure access to cloud applications. In essence, the identity is the core part of any virtualized CC system. Indeed, authentication attacks can lightly occur in cloud environments due to the weak mechanism of username and password that users still employ. As a result, authentication cloud attacks such as brute-force and dictionary attacks are the most common [31]. In this attack, the attackers target the mechanisms used by the user to authenticate the system [33],[34].

3) Structured Query Language (SQL) injection attack

Database and web servers make up a significant percentage of the systems within the cloud environment. The main goal of this type of attack is to steal user information from the web application, such as usernames and passwords or even credit cards, by injecting malicious code into the web application as a user input. If SQL-injection attacks are successful, then the attackers gain unauthorized access to the data and become able to remotely execute system commands as well as alter and delete the standard database design [35],[36].

B. Security attacks on PaaS cloud layer

As discussed, in PaaS, the user controls the applications that run in a cloud environment, but the cloud provider controls the hardware, network substructure, and operating systems. However, lack of validation, anonymous signs, and service fraud are major issues in PaaS [30]. We discuss famous types of security attacks on the PaaS cloud layer below.

1) Phishing attacks

Phishing attacks affect both providers and users in the PaaS cloud model. This type of attack aims to retrieve personal information from a legitimate user by manipulating a web link and redirecting the user to a spoofed link. In CC, phishing attacks can be classified into two categories. The first is an abusive behavior, in which an attacker hosts a phishing attack site on cloud by using one of the cloud services; the second involves hijacking the accounts using traditional social-engineering techniques [34].

2) Port Scanning Attack

The port scan is a very famous attack. The main aim of port scanning attack is to access to the resources in a cloud network. In this attack, the attacker use open ports address that belong to a connection to gain exact information about the working environment and running application processes. Consequently, the attacker exploit this information an exploit the vulnerabilities to perform the actual attack, since it's executed after scanning port phase [36],[37].

3) Man-in-the-middle attack

A Man-in-the-Middle attack is a major security issue that occurs when an attacker is placed between two parties in a cloud environment. This type of attack aims to access sensitive information being shared. However, if the communication channel is not secure between two parties (including providers), the attack can take place in an ongoing communication [38].

4) Metadata spoofing attack

Metadata is "data about data." In other words, it contains confidential and sensitive information. The descriptions of service functionality and details, for example, are stored in a Web Services Description Language (WSDL) file; an attacker may seek to access this file and apply modifications or delete operations. In this type of attack is possible if the attacker at delivering time succeeds to interrupt the service invocation code in the Web Services Description Language file [39].

C. Security attacks on IaaS cloud layer

The security concerns at the virtualized level are major securities threats to the IaaS computing environment. As previously discussed, in CC, available infrastructures include a collection of several computers, VMs, and storage resources to store important information such as confidential information and data documents. On this layer, the developer has better control over the security because there is no security hole in the virtualization manager [30]. Moreover, sharing physical resources of a host among virtual machines through a hypervisor abstraction layer is enabled by the virtualization. We describe some major security attacks on the IaaS cloud layer, as elaborated below.

1) Cross-virtual-machine attacks (Side channel attacks)

In the cloud environment, virtual machines (VMs) are easily accessible by the tenant users. Accordingly, they are the most vulnerable part of the virtualized system. Side-channel attacks are likely one of the most challenging types of attack in a cloud environment. These attacks are meant to extract confidential information from a victim's VM by exploiting side-channel information such as time, cache, heat, and power. This information is retrieved from the cryptographic software that is neither the plaintext to be encrypted nor the cipher text resulting from the encryption process [40]. Placement and extraction are the main steps in side-channel attacks.

2) VM rollback attack

Basically, in a VM rollback attack, the attacker takes advantage of a VM from an old snapshot and runs it without the user's awareness. The attacker can get the password for the VM by launching a brute-force attack, even if the guest operating system has a restriction on the number of failed trials. Moreover, the attacker can change users' permissions using rollback, a permission control module [41].

3) VM escape attack

The attacker interacts directly with the hypervisor to break the isolation layer. Another major issue at the VM level is a VM escape attack, which is malicious code that can interfere with the hypervisor or other guest VMs. In this type of attack, the attackers attempt to break down guest operating systems or gain access to the memory in order to access the hypervisor or penetrate the functionalities [34]. In essence, this breaking of the guest operating system is called an escape. In addition, the attacker gains access to the memory that is beyond the access of the compromised tenant VM and can read, write, or execute its contents. Furthermore, if successful, the attacker can control the entire guest operating system because the hypervisor is compromised [42].

Table II presents several security attacks over various cloud-service delivery models and their effects on the cloud (including some solutions). These categories are attacks, affected cloud services, effects, and finally, the solutions. Table II shows that several attacks have been applied to different cloud services and the most common attack in the CC environment is a DoS attack.

TABLE II. TYPES OF SECURITY ATTACKS

Attacks	**Affected Cloud Services**	**Effects**	**Solutions**
DoS	SaaS, PaaS, and IaaS	Service availability is affected; a fake service may be created	• Using strong authentication and authorization. • Using a filter-based approach. • Using signature-based approach. • Using an intrusion-detection or intrusion-prevention system.
Authentication	SaaS	Affects privacy and integrity	• Using strong passwords and a better authentication mechanism. • Applying Service Provisioning Markup Language, Secure Assertion Markup Language, OAuth, and Extensible Access Control Markup Language standards to secure federated identities. • Encrypting communication channels to secure authentication tokens.
SQL Injection	SaaS	Malicious service is provided to users instead of valid service. Service integrity is affected.	• Avoiding use of dynamically generated SQL in the code. • Using appropriate filtration to sanitize the user input. • Using a proxy-based architecture to dynamically detect and extract user input.
Phishing	SaaS, PaaS, and IaaS	Affects the privacy of the user credentials that should not be revealed	• Using secure web links. • Identifying spam e-mails. • Not clicking on short URLs. • Not clicking when someone forces you to click.
Port Scanning	SaaS, PaaS, and IaaS	Abnormal behavior of the service; affects service availability	• Using a time-independent feature set. • Using packet counts and neural networks. • Evolving TCP/IP packets. • Capturing packets. • Using firewalls.
Man in the Middle	SaaS, PaaS, and IaaS	Affects the data privacy and security.	• Requiring a proper Secure Socket Layer architecture. • Using an encryption and decryption algorithm. • Using an Intrusion Detection System.
Metadata Spoofing	SaaS and PaaS	Abnormal behavior of the service; affects the privacy of the service.	• • Encrypting information about service functionality and other details. • Requiring strong authentication to access files.
Cross-VM	IaaS	Allows an attacker to gain control over another user's VM.	• Using a virtual firewall. • Using encryption and decryption.
VM Rollback	IaaS	Allows an attacker to gain control over another user's VM.	• Using suspend and resume.
VM Escape	IaaS	Enables access to the credentials and control of another user.	• Monitoring hypervisor activities. • Requiring VM isolation. • Using a secure hypervisor. • Configuring the host/guest interactions.

VI. CONCLUSION

Cloud Computing security is an essential aspect of computer security, and it poses a major challenge to its widespread adoption because the fact that CC services are essentially based on Internet connection makes them vulnerable to a variety of attacks and security threats that may result in either light or severe impacts. In this paper, we reviewed the significant attacks threatening the security of Cloud Computing; moreover, we provided solutions and possible countermeasures to serve as a reference for comparative analysis.

REFERENCES

[1] Mell, P. and Grance, T. (2018). The NIST Definition of Cloud Computing. [online] National Institute of Standards and Technology | NIST. Available at: https://www.nist.gov/ [Accessed 15 Nov. 2018].

[2] Gupta, B. and Badve, O. (2016). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. Neural Computing and Applications, 28(12), pp.3655-3682.

[3] Chowdhury, R. (2014). Security in Cloud Computing. International Journal of Computer Applications (0975 – 8887), Volume 96– No.15, June 2014.

[4] D. Q. L. Shilpashree Srinivasamurthy, "Survey on Cloud Computing Security," Indiana University , US.

[5] Kumar, S. and Goudar, R. (2012). Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey. International Journal of Future Computer and Communication, pp.356-360.

[6] Nazir, M. (2012). Cloud Computing: Overview & Current Research Challenges. IOSR Journal of Computer Engineering, 8(1), pp.14-22.

[7] Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), pp.583-592.

[8] HUANG, W., GANJALI, A., KIM, B., OH, S. and LIE, D. (2015). The State of Public Infrastructure-as-a-Service Cloud Security. ACM Comput. Surv. 47, 4, Article 68 (June 2015), 31 pages.

[9] Cdr Nimit Kaura, W. and Col Abhishek Lal, L. (2017). SURVEY PAPER ON CLOUD COMPUTING SECURITY. In: International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS).

[10] Flavio, Lombardi, Pietro, Roberto Di, 2011. Secure virtualization for cloud computing. J. Network Computer. Appl. 34 (4), 1113–1122.

[11] Jiang, Yexi, Perng, Chang-shing, Li, Tao, Chang, Rong, 2012. Self-adaptive cloud capacity planning. In: Proceedings of the 2012 IEEE Ninth International Conference on Services Computing (SCC). IEEE, pp. 73–80.

[12] Ouedraogo, Moussa, Mignon, Severine, Cholez, Herve, Furnell, Steven, Dubois, Eric, 2015. Security transparency: the next frontier for security research in the cloud. J. Cloud Computing 4 (1), 1–14.

[13] Fernandes, Diogo A.B., Soares, Liliana F.B., Gomes, João V., Freire, M.ário M., Inácio, Pedro R.M., 2014. Security issues in cloud environments: a survey. Int. J. Information Security 13 (2), 113–170.

[14] Sumitra, B., Pethuru, C.R., Misbahuddin, M., 2014. A survey of cloud authentication attacks and solution approaches. Int. J. Innov. Res. Comput. Commun. Eng. 2 (10).

[15] Fotiou, Nikos, Machas, Apostolis, Polyzos, George C., Xylomenos, George, 2015. Access control as a service for the Cloud. J. Internet Serv. Appl., ISSN 1869-0238

[16] Choi, Junho, Choi, Chang, Ko, Byeongkyu, Choi, Dongjin, Kim, Pankoo, 2013. Detecting web-based DDoS attack using MapReduce operations in cloud computing environment. J. Internet Serv. Inf. Security 3 (Issue 3⁄4), 28–37.

[17] Kim, Jin-Mook, Moon, Jeong-Kyung, Hong, Bong-Hwa, 2013. An Effective Resource Management for Cloud Services using Clustering Schemes.

[18] N. Kajal, N. Ikram, and Prachi, “Security threats in cloud computing,” International Conference on Computing, Communication & Automation, 2015.

[19] A. Behl, “Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation,” 2011 World Congress on Information and Communication Technologies, 2011.

[20] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” The Journal of Supercomputing, vol. 63, no. 2, pp. 561–592, 2012.

[21] CSA: "The notorious nine: Cloud computing top threats in 2013." Top Threats Working Group, 2013.

[22] N. Amara, H. Zhiqui, and A. Ali, “Cloud Computing Security Threats and Attacks with Their Mitigation Techniques,” 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.

[23] A. Tripathi and A. Mishra, “Cloud computing security considerations,” 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2011.

[24] N. Aawadallah, “Security Threats of Cloud Computing,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 3, no. 4, pp. 2393–2397, 2015.

[25] Duncan, A. Creese, S. Goldsmith, “Insider attacks in cloud computing,” In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 857–862. IEEE Computer Society,Washington, DC,USA, 2012.

[26] W. R. Claycomb and A. Nicoll, “Insider Threats to Cloud Computing: Directions for New Research Challenges,” 2012 IEEE 36th Annual Computer Software and Applications Conference, 2012.

[27] Panah, A. Panah, A. Panah, O. Fallahpour, “Challenges of security issues in cloud computing layers” Rep. Opin. 4(10), 25–29, 2012.

[28] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M. Freire, and P. R. M. Inácio, “Security issues in cloud environments: a survey,” International Journal of Information Security, vol. 13, no. 2, pp. 113–170, 2013.

[29] S. Ramgovind, M. M. Eloff, and E. Smith, “The management of security in Cloud computing,” in 2010 Information Security for South Africa, Johannesburg, South Africa, 2010, pp. 1–7.

[30] S. Iqbal et al., “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” J. Netw. Comput. Appl., vol. 74, pp. 98–120, Oct. 2016.

[31] 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, Jan. 2011.

[32] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “DDoS attacks in cloud computing: Issues, taxonomy, and future directions,” Comput. Commun., vol. 107, pp. 30–48, Jul. 2017.

[33] S. T.K and D. B, “Security Attack Issues and Mitigation Techniques in Cloud Computing Environments,” Int. J. UbiComp, vol. 7, no. 1, pp. 1–11, Jan. 2016.

[34] A. Singh and K. Chatterjee, “Cloud security issues and challenges: A survey,” J. Netw. Comput. Appl., vol. 79, pp. 88–115, Feb. 2017.

[35] T.-Y. Wu, C.-M. Chen, X. Sun, S. Liu, and J. C.-W. Lin, “A Countermeasure to SQL Injection Attack for Cloud Environment,” Wirel. Pers. Commun., vol. 96, no. 4, pp. 5279–5293, Oct. 2017.

[36] P. Deshpande, S. C. Sharma, S. K. Peddoju, and A. Abraham, “Security and service assurance issues in Cloud environment,” Int. J. Syst. Assur. Eng. Manag., vol. 9, no. 1, pp. 194–207, Feb. 2018.

[37] A. Akbarabadi, M. Zamani, S. Farahmandian, J. M. Zadeh, and S. M. Mirhosseini, “An Overview on Methods to Detect Port Scanning Attacks in Cloud Computing,” p. 6.

[38] A. Singh and D. M. Shrivastava, “Overview of Attacks on Cloud Computing,” vol. 1, no. 4, p. 3, 2012.

[39] R. Anitha, P. Pradeepan, and P. Yogesh, “Data Storage Security in Cloud using Metadata,” p. 5, 2013.

[40] S. Anwar et al., “Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey,” J. Netw. Comput. Appl., vol. 93, pp. 259–279, Sep. 2017.

[41] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: A survey,” J. Netw. Comput. Appl., vol. 77, pp. 18–47, Jan. 2017.

[42] Yubin Xia, Yutao Liu, H. Chen, and B. Zang, “Defending against VM rollback attack,” in IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012), Boston, MA, USA, 2012, pp. 1–5.