# SECURITY THREATS AND ATTACKS IN CLOUD

**Asma Mohammed, Jamilah Al khathami and Wajdi Alhakami**

Taif University, College of Computers and Information Technology, Taif, Saudi Arabia

**Summary**
The amount of information and data in the digital era is increasing tremendously. Continuous online connectivity is generating a massive amount of data that needs to store in computers and be made available as and when required. Cloud computing technology plays a pivotal role in this league. Cloud computing is a term that refers to computer systems, resources and online services that aim to protect and manage data in an effective, more efficient and easy way. Cloud computing is an important standard for maintaining the integrity and security of sensitive data and information for organizations and individuals. Cloud security is one of the most important challenges that the security of the entire cloud system depends on. Thus, the present study reviews the security challenges that exist in cloud computing, including attacks that negatively affect cloud resources. The study also addresses the most serious threats that affect cloud security. We also reviewed several studies, specifically those from 2017-20, that cited effective mechanisms to protect authentication, availability and connection security in the cloud. The present analysis aims to provide solutions to the problems and causes of cloud computing security system violations, which can be used now and developed in the future.

***Keywords***
*Cloud Computing; Security; Attacks; Threats.*

## 1. Introduction

Cloud computing is one of the most inventive technologies of our times. Its most important goal is to supply one-of- a-kind services for users, including infrastructure, platform, or software program at viable costs for the users. However, cloud computing continues to be in its preliminary stage. The loss of standards, the security, and the interoperability problems hamper the increase of cloud computing. Thus, the quality of services is an essential attribute that must be met in cloud companies. However, measuring the high-satisfactory of cloud companies' security techniques is problematic because many cloud companies do not reveal their infrastructure to the customers [1].

Cloud computing is preferred by both organizations and individual users today because cloud architecture is based on remote instead of local servers. It offers dynamically scalable infrastructure or virtualized resources, platforms, and software programs in the form of services over the Internet. The technology is also a form of brand-new computing version. It proposes a transition from the conventional financial performance where the consumer is the proprietor of the software program and the hardware, towards a version wherein the consumer is turning into an easy tenant of services.

These services could be the use of software programs, or the required hardware. In a cloud computing environment, the services are supplied as preferred utilities that may be leased and launched through customers via the Internet on the basis of on-call or pay-as-used version [2].

The Cloud Computing trend is growing unprecedentedly, more so with enhanced technologies of Grid Computing, Utility Computing, and Distributed Computing. Cloud provider companies which include, Amazon IBM, Google's Application, Microsoft Azure, etc., provide the cloud environment to the customers for developing programs and to access these programs from anywhere. Cloud information is saved and accessed in a far-flung server with the assistance of services supplied through cloud provider companies. In this context, providing security is the main issue because it is transmitted to the far-flung server over a channel (Internet). Thus, before enforcing cloud computing in an organization, it is important to address the security-specific concerns first [3].

Security is the most elemental prerequisite for availing the benefits of cloud computing. In fact, achieving the desired level of security is indexed as the most crucial and demanding mission by the practitioners. The cloud companies are consistently working on mechanisms to ensure that they have got suitable security elements. Providing optimum data security is the foremost priority of these organisations. Data security is protecting the safety and processing of personal information from unlawful entry, alteration, or interruption [4].

The present study is an attempt to analyse the research endeavours that have been done from 2017-20 in the context of security concerns and attack threats in cloud computing and highlight the most effective solutions to counter these threats. To accomplish the stated objective, the rest of this study has been segregated into following sections:

Manuscript received January 5, 2021
Manuscript revised January 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.1.23

The second section presents the Background which explicates the definition and different types of cloud computing. The third section is on security challenges in cloud computing in which we have enlisted the major problem areas and the most important controls that must be provided in a cloud computing system in order to be more secure. The section also discusses the types of threats and attacks, methodologies and appropriate solutions to minimise the damages. The fourth section is a collation of several studies that have dealt with methodologies to reduce threats and attacks that compromise the security of cloud computing. Among them are studies related to authentication, connection security and availability in the cloud environment. The fifth section details the discussion on two specific studies done by the author in the context of security in cloud environment and the most important algorithms that the author used to increase cloud security. Finally, section sixth concludes the study.

## 2. Background

Cloud Computing technology provides programs, computing capacity, storage tools, and other such services to the users [5]. Cloud computing is a version for allowing convenient *on-call- network* to gain access to a shared pool of configurable computing sources (e.g., networks, servers, storage, programs, and services) that may be unexpectedly provisioned and launched with minimum control attempt or service issuer interaction. The demand and the use of cloud computing technology have seen a phenomenal increase in the present-day digital world. Hence, it has become even more essential to work in a successive manner and ensure that the users of cloud computing do not become the targets of attackers [6].

The National Institute of Standards and Technology (NEST) defines cloud computing as a version that gives *convenience- on-call* for providers, ubiquity, and admission to shared sources with minimum administrative attempt. Cloud computing increases organizations and companies' capacity to fulfil purchaser demands, gives services without the need for software program licenses, and train or purchase carriers' infrastructure. Users use servers (e.g., *iCloud, Dropbox*) to get admission to information that can be saved everywhere and anytime [7].

Cloud computing is a brand-new idea of computing technology that uses the net and far-flung servers to keep information and programs. This system lets the customers secure the value of hardware deployment, software program licenses, and system maintenance. It gives dramatically scalable and virtualized sources, bandwidth, software programs, and hardware on call for customers. The customers are capable of using programs or services in the clouds for the use on the net. Users can generally connect with clouds through internet browsers or internet services. Although cloud computing gives many benefits to the customers, it has numerous security issues [8].

Cloud computing gives hardware and software program components and sources through the net [6], where cloud computing presents a flexible and cost-powerful solution for lots Internet services [5]. By using cloud service, customers switch a load of software program installation, information maintenance, infrastructure, and storage space to the cloud providers. These centre's supply their customers the possibility to store, collect, and share information in an obvious way with different customers [9].

There are four types of cloud. These include: Public, Private, Community and Hybrid Cloud.

**1)Public Cloud:** This is one of the clouds in which cloud services are available over the Internet to the clients through a provider. It gives them a management mechanism. The services are either free of cost or depend upon a pay-per-use model [9]. This cloud is much less stable than different models since all the programs and information can be accessed by the public and is available through the Internet [1].

**2)Private Cloud:** This gives some of the public's advantages. However, the main difference between the two is that records are successfully controlled inside the organization by the consumer without the network band width limits [9]. Private cloud refers to a devoted cloud this is handled internally or with the aid of using a third-party and may be hosted usually on-premises or maybe externally [1].

**3)Community Cloud:** This type of cloud is controlled to use a collection of origin servers Members who share a cloud get admission to information [9], the physical infrastructure is managed and shared with the aid of using numerous companies and is primarily based on a community of interest [1].

**4)Hybrid Cloud***:* This is a combination of public and personal cloud. It also can be defined as more than one cloud system linked in a manner that makes it smooth to transport programs and information from one system to another [9], integrate or more significant extraordinary cloud infrastructures. This cloud must be related to using a well-known technology for information and program portability [1].

## 3. Literature review

Protecting data and information for institutions and individuals in the cloud environment is of utmost importance. In this section, we have presented studies that have cited several solutions that would increase protection, authentication, secure communication, and availability in order to create a more integrated and ideal cloud environment.

### 3.1 Security

Moving sensitive information to the cloud includes shifting the management of the information to the provider. Therefore, the security and confidentiality of facts turn into the central issue of information protection, and authentication in cloud computing. This is similar to protection and privacy for the information in conventional environments. However, establishing multi-location cloud computing, information protection and privacy entails additional risks [1]. The foremost priority is to guard the consumer's facts against display in cloud computing. In this context, Sinai Pearson recommend a layout system of cloud computing services which ensured that the consumer's message and facts related to commercial enterprises would not be leaked out. The layout is based on the following precepts:

- Transmit and save a person's records as less as possible. After systemic analysis, the cloud computing programs will acquire and save the full vital records only.
- Security measures can save consumers unauthorized access, copying, usage, or enhancing private records
- Achieve the two-pronged target of consumer management to the best degree. Firstly, it is crucial to permit the consumer to govern the critical private records as much as possible. Secondly, minimize the control of private records through a dependent on the third party. Allow customers to make a choice. Users have the proper means to choose the private records that need to be saved.
- Restrict the reason for the use of information. Personal records must be used and dealt with through the individual with a unique identity for a unique reason, and the proprietor of records must be notified earlier before using them.
- Establish remarks mechanism to ensure that the service's safety suggestions and specific measures can be supplied to the consumer promptly.
- The abovementioned concepts can maximize the security of the consumers' records [12].

### 3.2 Threats

Security in the cloud computing is the primary mission and it lack is retarding the proliferation of cloud computing. Understanding the different aspects involved in cloud computing is a critical issue, and several organizations and popular companies have been working on this. Cloud security Alliance (CSA), NIST, ENISA, among several others, are some of the leading companies operating in the domain of cloud security. These organizations have cited several recommendations and suggested guidelines for working in a secure cloud environment. Among all the above organizations, the Cloud Security Alliance is solely dedicated to cloud protection. Many of the big files have already been posted to CSA for cloud security. Moreover, to spread awareness about the main and current threats, CSA also posted a document on the top threats for the users. CSA posted its first document, titled- 'Top Threats to Cloud Computing V1.0' in 2010. However, based on further investigations on the alternate methodologies that attackers were using, and after observing the present-day security trends in cloud computing, CSA posted yet another dossier in 2013. The document was titled, 'The Notorious Nine Cloud Computing Top Threats in 2013'. In this examination, CSA reviewed hundreds of articles associated with cloud threats and visited unique websites. The organization diagnosed the primary threats on cloud computing, which have a vast effect in cloud computing. After a through scrutiny, the specialists identified nine crucial threats to cloud security ranked as per the level of severity [13]:

**Table 1:** Threats in Cloud Computing.

| Threats | Approaches |
|---|---|
| Data Breaches | Once the records are accessed by any entity, aside from the owner, it should be referred to as an information breach. Multifunctional cloud computing architecture provides additional security vulnerability if it is not well designed. In this threat, the adversary can use the digital machine's aspect channel timing records to extract the personal cryptographic key utilized in other's VM at the identical physical server [13]. |
| Data Loss | This danger will increase within the cloud because of the cloud environment's architectural or operational characteristics (e.g., insecure APIs, shared environment.) [14]. |
| Account Hijacking | Phishing, fraud, and exploitation are well-known problems in IT. The cloud provides a brand-new size to this danger: Such attacks mean that an attacker profits by gaining access to the users' credentials, in such a case the attacker can listen in on the users' activities and transactions, manage records, go back to falsified records, and redirect the customers [14]. |
| Insecure APIs | Fixed APIs to control and interact with cloud services are generally exposed (provisioning, monitoring.). Cloud services' protection relies upon the security of the fundamental APIs [14]. |
| | In the denial of services, illegitimate customers use cloud sources and deny valid customers the access to the sources. |

| | |
|---|---|
| Denial of Services | Dispensed Denial of Services (DDoS) attacks often occur in cloud computing [13]. |
| Malicious Insiders | This is amplified inside the cloud with the aid of using "the convergence of IT services and customers beneath a single control domain, mixed with a well-known loss of transparency into issuer's system and procedure [14] |
| Abuse of Cloud Services | IaaS companies deliver the phantasm of limitless, network, storage capacity and compute. But IaaS services Hosted botnets, trojan horses, and the attack security application [14]. |
| Insufficient Due Diligence | Many customers are deciding on the cloud because of significant infrastructure, minimal premature cost, and the safety supplied to use the cloud. Considering the massive increase in capacity, many new cloud issues have emerged and keep emerging daily. Consequently, it is vital to monitor the workings of the cloud's issuer and assess the safety supplied, regulatory compliance, etc. Necessary agreement associated with the availability of records should also be checked for avoiding any disputes [13]. |
| Shared Technology Issues | IaaS companies supply their services in a scalable manner with the aid of using the shared infrastructure. Monitor environment for unauthorized changes/activity [14]. |

### 3.3 Attacks

Cloud resources in the cloud environment are an attractive ground for cyber criminals due to the tremendous resources available in the central place. These criminals can access cloud resources from any part of the world at any time, even the use of the device does not restrict the use of cloud resources. Thus, the resources of the cloud are huge. The ones at the opponent's disposal pose a great threat to the cloud and to the web users. These attackers are working to exploit the resources of the cloud to conduct many cyber-attacks.

McAfee and Guardian analysis revealed a sophisticated attack that specifically targets financial services.

In the past, cybercrime was believed to be confined to Europe, but studies revealed that these attacks have reached other parts of the world also, including the United States and Colombia. These attacks are automatic and targeted. The accounts with a huge balance are the prime exploits, for example, the credit unions, the major global banks and the regional bank. Through these fraudulent attacks, the attackers have been where able to pilfer 78 million USD from various accounts of financial institutions [11].

In the ensuing table II, we have enlisted numerous security attacks on cloud service transport models and their outcomes at the cloud (such as a few solutions). These categories are: Attacks and the affected cloud services, outcomes, and finally, the solutions. As per the data in table II, it is evident that numerous attacks were carried out on specific cloud services and the maximum attacks in the CC environment were that of DoS attacks [25]

**Table 2.** Types of Attacks on The Cloud

| Ref | Attacks | Year | Cloud Service | Approaches |
|---|---|---|---|---|
| [25] | Dos | 2019 | SaaS, IaaS, and PaaS | The attacker sends thousands of request packets to the victim, leading to affecting the availability service and creating a fake service. To avoid this attack, detection, strong authentication and signature must be used. |
| [25] | Cross-Virtual-Machine Attacks | 2019 | IaaS | In this attack, the virtual system of some other consumer is controlled. by strong firewalls, encryption and decryption need to be used. |
| [26] | Authentication Attack | 2018 | SaaS | This attack is geared toward cracking passwords and unauthorized amendment of data. Strong passwords need to be chosen, biometrics are used, and encrypted Communication channels are also used to enhance stable authentication |
| [27] | SQL Injection | 2020 | SaaS | This attack pilfers data through internet servers. The attacker sends malicious code geared toward stealing passwords or usernames to get admission to databases and makes adjustments and deletions on the users' data. |
| [27] | Man-in-the-middle attack | 2020 | SaaS, PaaS, and IaaS | It aims to access private and sensitive information. Suitable solutions for this attack are to use an encryption and decryption algorithm and use the intrusion detection system. |
| [28] | Port Scanning Attack | 2020 | SaaS, PaaS, and IaaS | It is very common where the port addresses belonging to a connection are used within a cloud environment. The intent is to access accurate information about the work environment and how the application is running. To avoid this attack, TCP / IP packets must be developed. Packet capture. The use of neural networks, out-of-time features, firewalls is also effective. |
| [29] | Phishing Attacks | 2020 | SaaS, PaaS, and IaaS | Phishing attacks target both service providers and users with the purpose of gaining access to private and sensitive information such as passwords and usernames by sending fake messages or links via the web. To avoid this attack, the users should not open random links. Users should also not open anonymous emails and use secure websites only. |
| | | | | Metadata is "*records' information*." In other words, it consists of private and sensitive |

| | | | | |
|---|---|---|---|---|
| [30] | Metadata Spoofing Attack | 2019 | SaaS and PaaS | records. The descriptions of provider's capability and details, an attacker may also be searching for to access this fi le and observe modifications or delete operations. Encrypting information about service functions is one of the solutions to protect this information. |
| [31] | VM Rollback Attack | 2019 | IaaS | Allows the attacker to manage some other user's VM by using suspend and resume. |
| [31] | VM Escape | 2019 | IaaS | The attacker can manage some other user's system and get admission to the data. To keep away from this attack, consumers need to use a secure hypervisor and display its activities continuously. |

### 3.4 Literature sources in the context of Protection

Literature resources in the context of Authentication: Researchers presented this study [15] in 2019. mainly aims at hiding information of the image by Using the hidden image authentication and its algorithm in the cluster cloud system, where this algorithm is applied to the picture in a public cloud platform, so the SSIA algorithm is added to the image information using blowfish algorithm and genetic operators. Blowfish symmetric block encryption is applied to the image and then the image information is completely encrypted. This authentication algorithm provides improved security compared to the traditional blowfish algorithm. In figure 1, an illustration of the proposed system structure in this study. [15]

In 2017, focused on creating a secure cloud system Using multiple levels of hash and encryption along with multi-factor authentication, a CloudSim emulator was used, through which a cryptographic system (HCS) was used, which combines the benefits of symmetric and asymmetric encryption, as the cloud ecosystem that was proposed is a security for data privacy by following systems Encryption at different levels. By using this system all coding techniques are enhanced during the design of that system was developed by including the process of authentication that allowed the feature of One Time Password (OTP) [16].

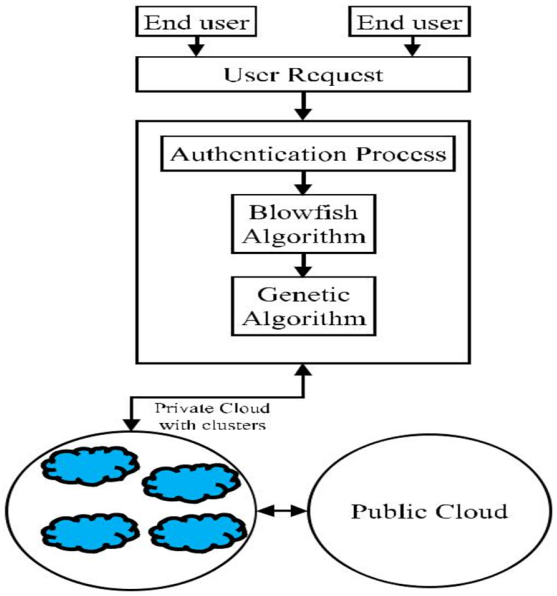


**Fig. 1.** The System Architecture Proposal [15].

In 2017, a group of researchers presented a methodology of using identity management, authorization, and access control. This methodology could achieve strong levels of authentication in cloud computing [17].

Secure Communication: Security is seen as a common barrier in adopting the cloud mode of internet realism [18]. Many studies have been conducted to make a connection more secure within any cloud environment. In this context.

In the study [18], Connectivity Security has been diagnosed as one of the most crucial problems of cloud computing wherein resolving such a problem might bring about a regular increase in the use and recognition of cloud computation. The study constructed a cellular advert hoc network mobility model framework for the usage of cloud computing that offered stable Internet of Things communique among intelligent devices. This contribution was a brand-new methodology for ensuring stable communique with the 5G network of intelligent devices. The suggested method is a correct and robust simulation and may be carried out in an Internet of Things structure. These studies might create novel connectivity architecture to deal with the problem of stable communiqué among intelligent devices in 5G networking.

In the study [19], It has been carried out a complete look at to study the capacity threats confronted with the aid of using cloud customers and decided the compliance models and security controls that must be in the area to control the risk. This system examines how to expand a semantically wealthy ontology to version the security threats, cloud protection guidelines, and controls and detailed the issuer records. Also been advanced a smooth to apply cloud security coverage software for customers who

are making plans to transport their documents to the cloud however are hesitant because of security worries as they will now no longer be aware of the security controls. As a part of this ongoing work, they studied different IT compliance models that can be relevant, withinside the cloud paradigm and decide if they must be integrated with cloud security software. Researchers additionally worked on growing guidelines to cause over the ontology to higher fit compliant providers. In the figure 2, the relationship between the safety controls and the security compatibility classes described by the ontology in this study is described.

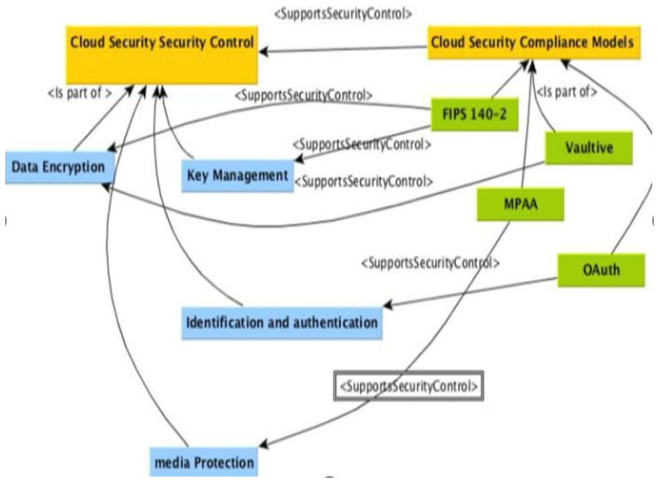


**Fig. 2.** The Image Proposed in Study [19].

Literature resources in the context of Availability: Reliability and excessive availability continue to be a prime challenge in disbursed systems. Providing exceptionally dependable cloud computing services is crucial for keeping consumers' faith and stopping losses. Although numerous solutions were proposed for cloud availability and reliability, there is no complete research that covers all specific components of the problem [20].

The paper presented [20] a reference Roadmap' of reliability Customers decide upon the compliance models and security controls that must be in the area to control the risk. This system examines how to expand a semantically wealthy ontology to categories the security threats, cloud protection guidelines, and controls and monitor the issuers' records. The system also provides advanced cloud security coverage software for customers who are making plans to transport their documents to the cloud but are hesitant to do so because of security worries as they will now no longer be aware of the security controls. The authors analyzed different IT compliance models that can be relevant in the cloud paradigm and decided if they must be integrated with cloud security software. Furthermore, the researchers also provided guidelines of the ontology that would be more compliant and enable excessive availability in cloud computing environments. The system was divided into four steps, which are defined as when, how, where, and which one. As each step was proposed from a proposed system, where two basic papers were presented and a proposal for this system was a good picture of the system for high reliability and the problem of availability within computing environments. figure 3, shows the big, proposed reference roadmap for solving the high availability problem in the cloud computing environment.

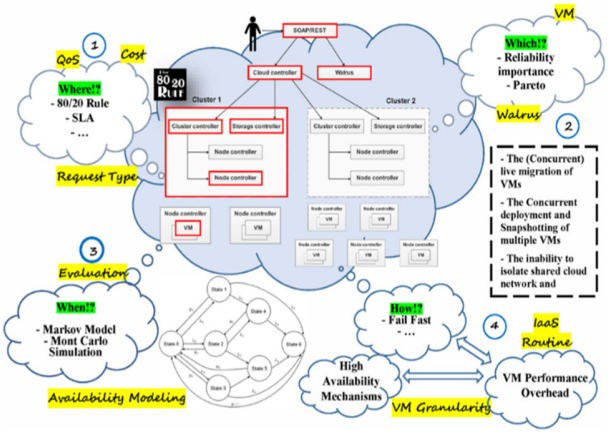


**Fig. 3.** The Image Proposed in Study [20].

This paper [21] proposed the architecture for excessive availability that can dynamically optimize the provisioning technique primarily based on the provider's characteristics. The proposed architecture was established via an implementation system based on *OpenStack.* The system was capable of obtaining the goal of availability and optimize on the resources at the same time. The architecture was able to automatically configure the supply technique in line with provider's characteristics. The study thus gave a template for a cloud architecture that could automatically configure fault detection and fault restoration strategies associated with numerous characteristics of the providers.

In 2020, a group of researchers designed a new approach that aims to predict the time periods available in the data node, based on the use of an artificial neural network (ANN). This neural network predicts the time when cloud resources are available after several experiments on more than one data node. This method has succeeded. It has been proven to be 98% effective.[22]

### 3.5 Literature sources in the context of Detection:

In this research paper [23], a complete survey of current technology turned into a discovery of unique kinds of intrusion in the cloud environment. A VMI- based intrusion detection technique was advanced to leverage

virtual simulation concepts. The outcomes of this survey suggested the pros and cons of every category, technique, and method. The research applied the concept onto several other demanding situations in cloud computing to test the efficacy of the suggested technique.

In 2017, a study was presented in which a system called the C4 algorithm was presented. 5 aims to detect DDoS attacks. This system relies on the use of C4.5, which is an algorithm used alongside other techniques such as machine learning techniques and signature detection techniques. Focus on Layer 3 and Layer 4 that a DDoS attack targets in a seven-layer OSI model. This study resulted in high accuracy in detecting dumping attacks and making the cloud environment more secure and reliable.[24]

## 5. Discussion

With the development of cloud computing and its availability for all segments of society, it must have policies that protect it from attacks and threats that may be exposed to it at any time and from any side. Therefore, encryption is a necessary policy through which a more secure cloud computing environment can be provided. It is considered AES encryption (Advanced Encryption Standard) algorithm is symmetric in the sense that it uses the same key to encrypt and decrypt information. So, this secret key is only shared between the sender and the receiver. It is one of the most popular means of encrypting important and sensitive data, as it is used by famous organizations such as Apple and Microsoft for its ability to resist attacks and intrusion, such as its use in encrypting passwords using AES 256-bit encryption to protect user data, as well as using it to encrypt sent messages such as using it in the WhatsApp application. RSA was also one of the first asymmetric encryption algorithms to use different keys to encrypt and decrypt data. Using both the private key (only the owner knows it) and the public key (others on the same network know it), information that as it is encrypted with the public key, it cannot be decrypted by its private key. dealing with RSA system is easier than the DES system, although It is less fast and less secure. One of the basics of this algorithm is that it contains a digital signature that identifies the sender and confirms his identity. Therefore, it is very important to encrypt sensitive and important data and information before saving them in the cloud for more security and privacy.

## 6. Conclusions

This research study essentially discussed about the compelling issue of security in cloud computing and presented a concerted review on all aspects associated with this issue. Besides understanding the concept of cloud computing, its types and services that benefit both the organizations and individuals, the study enumerated the challenges that exist in the cloud environment. Security and the principles that must be available in a cloud computing system to be more secure are a pivotal need today. Moreover, attacks and threats of all kinds are also affecting the cloud's infrastructure. Many solutions have been developed to contain and minimize the impact of these invasions on the privacy and security of cloud users. The present paper attempted to compile a repository of several methodologies suggested by other researchers working in the domain of cloud computing. In this row, we specifically identified key solutions cited for authentication, security of the connection and the availability of resources within the cloud computing environment. Our goal in this paper was to learn about cloud computing technology and how to make it more secure through the use of methodologies that make the cloud environment more integrated and ideal at present and in the future.

## References

[1] Leila, B., Abdelhafid, Z., & Mahieddine, D. (2017, April). New framework model to secure Cloud data storage. In Computer Science On-line Conference (pp. 44-52). Springer, Cham.

[2] Jin, C., Gohil, V., Karri, R., & Rajendran, J. (2020). Security of Cloud FPGAs: A Survey. arXiv preprint arXiv:2005.04867.

[3] Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. Procedia Computer Science, 48, 204-209.

[4] Kacha, L., & Zitouni, A. (2017, September). An overview on data security in cloud computing. In Proceedings of the Computational Methods in Systems and Software (pp. 250-261). Springer, Cham.

[5] Benabied, S., Zitouni, A., & Djoudi, M. (2015, June). A cloud security framework based on trust model and mobile agent. In 2015 International Conference on Cloud Technologies and Applications (CloudTech) (pp. 1-8). IEEE.

[6] Mathariya, S. Implementation of security architecture in Cloud computing using ECC and BLOWFISH algorithm.

[7] Dheyab, O. A., Turki, A. I., & Rahmatullah, B. (2018). Threats and Vulnerabilities Affecting the Adoption of Cloud Computing in Iraq. The Journal of Social Sciences Research, 599-606.

[8] Jamil, D., & Zaki, H. (2011). Security issues in cloud computing and countermeasures. International Journal of Engineering Science and Technology (IJEST), 3(4), 2672-2676.

[9] Abdul-Jabbar, S. S., Aldujaili, A., Mohammed, S. G., & Saeed, H. S. (2020). Integrity and Security in Cloud Computing Environment: A Review. Journal of Southwest Jiaotong University, 55(1)

[10] De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. Future Internet, 11(6), 127.

[11] Qi, Q., & Tao, F. (2019). A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE Access, 7, 86769-86777.

[12] Kaur, R., & Kinger, S. (2014). Analysis of security algorithms in cloud computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 3(3), 171-176.

[13] Singh, J. (2014). Cyber-attacks in cloud computing: A case study. International Journal of Electronics and Information Engineering, 1(2), 78-87.

[14] Vaquero, L. M., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. Computing, 91(1), 93-118.

[15] Venkatraman, K., & Geetha, K. (2019). Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm. Automatika, 60(3), 314-321.

[16] Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 288-292). IEEE.

[17] Arora, A., Khanna, A., Rastogi, A., & Agarwal, A. (2017, January). Cloud security ecosystem for data security and privacy. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 288-292). IEEE.

[18] Alam, T. (2020). Internet of Things: A Secure Cloud-based MANET Mobility Model. IJ Network Security, 22(3), 514-520.

[19] Cloud security and compliance - A semantic approach in end to end securityArticle in International Journal on Smart Sensing and Intelligent Systems · September 2017 DOI: 10.21307/ijssis-2017-265 .

[20] Mesbahi, M. R., Rahmani, A. M., & Hosseinzadeh, M. (2018). Reliability and high availability in cloud computing environments: a reference roadmap. Human-centric Computing and Information Sciences, 8(1), 20.

[21] Yang, H., & Kim, Y. (2019). Design and Implementation of High-Availability Architecture for IoT-Cloud Services. Sensors, 19(15), 3276.

[22] Rayan, A., Alhazemi, F., Alshammari, H., & Nah, Y. (2020). Developing Cloud Computing Time Slot-availability Predictions Using an Artificial Neural Network. IEIE Transactions on Smart Processing & Computing, 9(1), 49-57.

[23] Mishra, P., Pilli, E. S., Varadharajan, V., & Tupakula, U. (2017). Intrusion detection techniques in cloud environment: A survey. Journal of Network and Computer Applications, 77, 18-47.

[24] Zekri, M., El Kafhali, S., Aboutabit, N., & Saadi, Y. (2017, October). DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech) (pp. 1-7). IEEE.

[25] Alhenaki, L., Alwatban, A., Alamri, B., & Alarifi, N. (2019, May). A survey on the security of cloud computing. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-7). IEEE.

[26] Chand, K. S., & Rani, B. K. (2018). Biometric Authentication using SaaS in Cloud Computing. International Research Journal of Engineering and Technology (IRJET), 5(2).

[27] Shunmugapriya, B., & Paramasivan, B. Protection Against SQL Injection Attack in Cloud Computing.

[28] Patel, R. V., Bhoi, D., & Pawar, C. S. (2020). Security Hazards, Attacks and Its Prevention Techniques in Cloud Computing: A Detail Review.

[29] Abusaimeh, H. (2020). Security Attacks in Cloud Computing and Corresponding Defending Mechanisims. International Journal of Advanced Trends in Computer Science and Engineering, 9(3).

[30] Desarkar, A., & Das, A. (2019). Encryption Algorithm for Data Security in Cloud Computing. Security Designs for the Cloud, Iot, and Social Networking, 1-18.

[31] Alhenaki, L., Alwatban, A., Alahmri, B., & Alarifi, N. (2019). Security in cloud computing: a survey. International Journal of Computer Science and Information Security (IJCSIS), 17(4).