International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (Apr-2021)

http://dx.doi.org/10.12785/ijcds/100152

Securing Cloud Computing: A Review

Zainab Salman[1] and Mustafa Hammad[1]

[1] Department of Computer Science, University of Bahrain, Sakheer, Bahrain

Received 1 Jul. 2020, Revised 30 Nov. 2020, Accepted 5 Feb. 2021, Published 21 Apr. 2021

Abstract: One of the latest technologies in the IT industry is cloud computing. Cloud computing is also called on-demand computing. This technology has high reliability, scalability, and performance. It has a relatively low cost compared to the traditional infrastructures. Cloud computing provides services over the Internet and it can assign many resources simultaneously to multi-users upon their request. In cloud computing, the main concern is security and trust. Many issues and challenges are related to the security of cloud computing. These issues in cloud computing mostly happen when the cloud is public, and the customer is not aware of where the data are stored on the Internet. In this paper, cloud computing security has been reviewed. A literature review has been done on previous studies from different perspectives. It shows that the studies have been conducted in securing cloud include using different security algorithms and encryption methods, using machine learning to make cloud computing more secure, and securing big data in cloud computing system. Moreover, a statistic of the previous studies, a taxonomy, and an analysis of existing studies have been discussed. In this analysis, some studies have been compared in terms of the methods and techniques used to secure the cloud computing system. Furthermore, future directions and conclusions of this review have been discussed based on existing studies and researches.

Keywords: Cloud Computing, Security

1. INTRODUCTION

Nowadays, cloud computing is being used in many industries and academic organizations related to IT. In addition, many individual users are starting to use it when they access the Internet. Cloud computing services are very easy to use, and they can be requested on demand whenever the user needs them. As a result, cloud computing is cheaper in cost. In addition, it is managed by the Cloud Service Provider. So, no need for management efforts. Examples of cloud computing providers are Amazon, Google, IBM, and Microsoft [1].

The cloud paradigm consists of five essential characteristics, three service models, and four deployment models [2]. The five essential characteristics are broad network access, rapid elasticity, resource pooling, on-demand self-service, and measured service. The three service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), and the four deployment models are public cloud, private cloud, hybrid cloud, and community cloud.

Although many studies have been conducted for securing the cloud, there are still some shortfalls and gaps in the cloud paradigm. The number of cyber-attacks is increasing as the technologies and tools are improving. Good security practices and measurements are needed to overcome these challenges and attacks. Consequently, many researchers have proposed different models and solutions for securing the cloud. Some researchers used encryption algorithms and methods to improve security. In addition, some researchers have used different machine learning techniques and optimization algorithms to add more features and sophisticated mechanisms to the security of the cloud. Furthermore, some studies have been done to secure big data that are used by many companies and users on the Internet.

This paper reviews cloud computing security in general. It provides a literature review on the previous works that have been done in securing the cloud from different perspectives. The literature review focuses on three main parts. First, encryption methods are used for securing the cloud. Second, used machine learning algorithms for cloud security, and third, securing big data in a cloud computing system. In each part, different studies are shown with different methods and techniques proposed by the authors. Moreover, a taxonomy and an analysis of the available studies have been discussed to provide a complete vision about the existing works in securing cloud computing systems. Furthermore, this paper presents security issues and challenges from different perspectives of cloud computing. It shows the security issues that are related to data centers, visualization, and the network which a cloud computing system is working on. In the end, this paper discusses the future directions for cloud computing security and a conclusion as a result of reviewing cloud computing security.

E-mail: zsalman@uob.edu.bh, mhammad@uob.edu.bh

The remaining sections of this paper are organized in the following structure: Section 2 explains essentials of a cloud computing. Section 3 illustrates a taxonomy of different studies in cloud computing security. Further, section 4 provides a statistic of researches that are interested in securing cloud computing. A literature review studied in section 5 that shows previous works in cloud computing security in three different fields. Section 6 presents a cooperative analysis on some of the previous works. Different challenges and issues are discussed in section 7. Section 8 suggests some future directions related to security of cloud computing, and finally section 9 provides some conclusion remarks that are based on reviewing different studies in cloud computing security.

2. Cloud Computing Essentials

Cloud computing has become one of the most popular technologies nowadays. Cloud computing means to store and access data or programs using the Internet from a remote location instead of using a local computer hard drive. This technology provides users with many benefits, such as reduced cost, increased agility, and flexibility. Therefore, many organizations, businesses, and governments have started to use it as an integral part of their computing system. When using an online connection, the user can access the data anytime, anywhere using any device. According to the National Institute of Standards and Technologies (NIST), the cloud model consists of five essential characteristics, three service models, and four deployment models. The essential characteristics and models for cloud computing are depicted in Figure 1 [2].

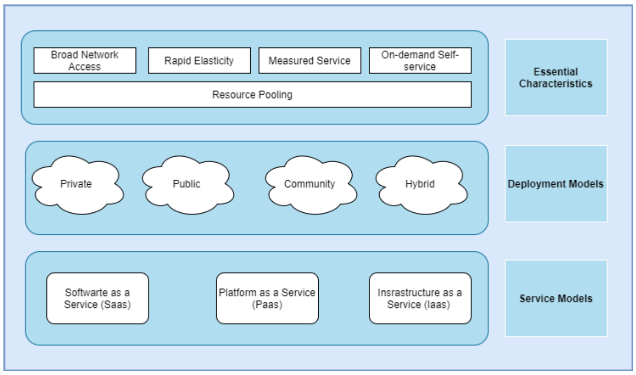

Figure 1. Essentials of a cloud computing system

As shown in Figure 1, the essentials of cloud computing are divided into three parts. They are essential characteristics, deployment models, and service models. If there is anything missing in any character or model, the system is not cloud computing.

Cloud computing has five major characteristics. First, the service provider should provide the consumer automatically with computing capabilities such as server time and network storage without any human interaction (On-demand Self-service). Secondly, any thick or thin client platform like mobile phones, laptops, and personal computers, should easily access the available capabilities over the network (Broad Network Access). Also, computing resources such as storage, memory, or network bandwidth are available to serve multiple customers at the same time. The resources are assigned and reassigned according to customer demand (Elastic Resource Pooling). Further, the capabilities should be rapidly provisioned to scale out and sometimes released to scale in. The consumer has an unlimited quantity of data that is always available (Rapid Elasticity). Finally, cloud systems control and optimize the usage of services and report it to both the consumer, and the provider of the service (Measured Service).

There are four major deployment models for cloud computing. They are Private Cloud, Public Cloud, Community Cloud, and Hybrid Cloud. In the private cloud, the infrastructure is provided for the exclusive usage of an organization. The organization or a third party or even some combination of both can manage the infrastructure. The private cloud may exist on the premises or not. In the public model, the cloud infrastructure is provided for open use and any user can use it. The public model can be owned, managed, and operated by a business or a government organization. It exists on the cloud provider side. In the community cloud, the infrastructure is shared by many organizations that have a common mission, policy, security requirements, and other concerns. The organizations or a third party can manage the community model, and it can be on or off the premise. Lastly, in the hybrid cloud, the infrastructure is a combination of two or more different cloud infrastructures (private, community, or public). These techniques bound together in a way to ensure data and application portability.

There are three kinds of services that are offered by cloud computing. They are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In SaaS, the consumer can access applications, which are running on a cloud such as a network, software, storage, and servers. In the PaaS model, the consumer has access to a complete ready-to-run package, which includes the programming languages, the libraries, and tools. The PaaS vendor provides everything and is responsible for management and maintenance. In the IaaS model, the consumer can access applications with the operating system. The consumer does not manage or control the infrastructure, but he has control over the operating system, storage, and limited access for selected networking components. The provider is responsible for maintenance. Examples of IaaS providers are Amazon Web Services (AWS), Microsoft Azure, and Google Compute Engine (GCE).

Cloud computing has a complex environment. Essential services and deployment models are needed. Furthermore, some actors are needed who are responsible for providing, maintaining, developing, or consuming cloud data. The actors are categorized into Cloud Service Users (CSUs), Cloud Service Provider (CSP), and Cloud Server Partners (CSNs). CSUs are the consumers of cloud computing and can be a user, a machine, or applications. CSP provides, delivers, manages, and maintains the service to the consumers. CSNs are those who provide support to the cloud system, such as an application developer or a content or equipment provider.

Cloud Computing has many advantages. One of its benefits which makes cloud computing attractive, is accessibility. When the documents and applications are on the cloud, the user can access data anytime and anywhere. The user does not need to be at his office to get access to his files. Another advantage is Scalability. Anytime the consumer needs more computing power, cloud computing can provide it instantly. In addition, there are no capital expenses only operational expenses. The user will pay as much as he uses. There is no maintenance cost nor management cost. Moreover, cloud computing provides more reliability by transferring the data from bad or offline devices to functional and working devices. Also, cloud computing promotes the concept of a green environment by multitenancy and visualization. All computing tasks can be done remotely with less computing hardware on-premise.

Cloud computing has some drawbacks. A major drawback is that the cloud-computing system depends on the Internet. If the user loses the connection to the Internet, he will lose the connectivity to the cloud. As a result, the user will lose access to the files and data. In addition, there is a concern about security because the data and programs are running on others' computing power. Further, the consumer may face some restrictions regarding the availability of some applications, platforms, or infrastructure. Restrictions depend on the vendor or the provider of the service because the consumer does not own the infrastructure totally. Another problem that may happen in a cloud computing system, is the interoperability of applications that exist on two or more different vendors. If the vendors or the providers do not cooperate appropriately with each other, they will not be able to offer the service to the consumer smoothly.

The security of the cloud is a major challenge in a cloud computing paradigm. The Cloud Service Providers (CSPs) are responsible for providing different security mechanisms to guarantee that the data and applications are accurately secured and can be used smoothly. Five major security objectives should be provided for any cloud computing system in terms of data, information, and computing services. They are Confidentiality, Integrity, Availability, Authenticity, and Accountability. Confidentiality is used to preserve authorized access and limitations on using data. Integrity protects data against inappropriate or illegal modification. Availability ensures reliable and timely access to data or information. Authenticity defines the source of data or a message and it defines the identity of the sender. Accountability is a security goal that defines the rule and responsibility of an entity in an organization.

3. Taxonomy Of Cloud Computing Security

In this section, a taxonomy of cloud computing security has been described according to the studies that have been reviewed. As Figure 2 shows, many studies have been conducted in different areas to solve the problems that are related to cloud computing security.

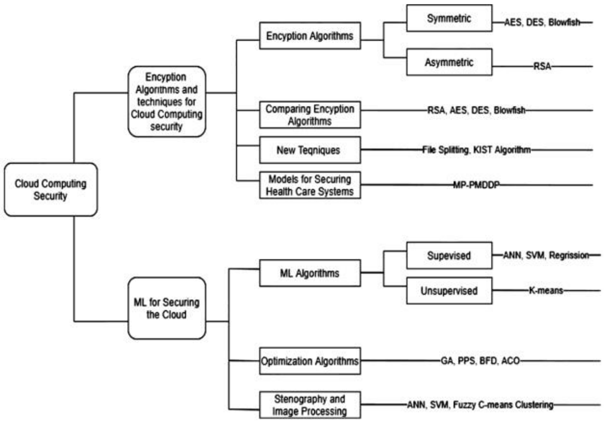
Cloud Computing Security
Encyption Algorithms and techniques for Cloud Computing security
Encyption Algorithms
Symmetric
AES, DES, Blowfish
Asymmetric
RSA
Comparing Encyption Algorithms
RSA, AES, DES, Blowfish
New Teqniques
File Splitting, KIST Algorithm
Models for Securing Health Care Systems
MP-PMDDP
ML for Securing the Cloud
ML Algorithms
Supevised
ANN, SVM, Regrission
Unsupervised
K-means
Optimization Algorithms
GA, PPS, BFD, ACO
Stenography and Image Processing
ANN, SVM, Fuzzy C-means Clustering

Figure 2. Taxonomy of cloud computing security

Figure 2 illustrates that the reviewed studies can be divided into two different categories. The first category includes the works that are related to different encryption techniques and algorithms to secure the cloud. The second category is related to those studies that used ML algorithms for securing the cloud. In addition, related methods and techniques for each sub-category have been addressed.

Different studies used different encryption algorithms and methods for securing the cloud. There are two main types of used encryption methods, symmetric and asymmetric. For the symmetric encryption algorithms, most of the studies used AES, DES, and Blowfish, whereas other studies used asymmetric encryption algorithms such as RSA. Some works compared the mostly used encryption algorithms in securing data like AES, RSA, Blowfish and DES algorithms and showed how they are different in case of the platform, key size, scalability, memory usage, encryption time, etc. Further, other techniques and algorithms have been used to protect the data such as using a split algorithm and folder lock to encrypt and decrypt the stored data. Moreover, the KIST algorithm has been proposed to encrypt the data while it is saved on the cloud. Some models have been proposed for securing Health care systems. Some authors proposed an MP-PMDDP (Map-Based Provable Multicopy Dynamic Data Possession) association to avoid document duplicates to question untrusted internet servers.

Machine learning is one of the most popular research fields. Many studies have addressed the security of the cloud using different ML algorithms. As Figure 2 depicts, some papers used ML for securing the cloud. They used supervised algorithms such as Artificial Neural Network (ANN), Support Vector Machine (SVM), and regression. Moreover, other studies used unsupervised ML algorithms like K-means Algorithm. Some papers used optimization algorithms in securing the cloud computing system. They used different intelligent algorithms like Parallel Particle Swarm Optimization (PPSO), Best Fit Decreasing (BFD) algorithm, Genetic Algorithm (GA), Ant Colony Optimization (ACO), etc. These algorithms can be used to optimize the results and utilize the efficiency of the cloud system resources. Furthermore, machine learning has been used in stenography and image processing for securing data or messages by embedding them into an image or video. Artificial Neural Network (ANN), and Support Vector Machine (SVM) have been used in such studies. In addition, some works used Fuzzy C-means Clustering to increase the efficiency and accuracy in their results.

4. Statistics of Studies in Cloud Computing Security

Many studies and surveys have been conducted related to securing cloud computing systems. SCOPUS database shows that a total of 21,657 documents have been generated in cloud computing security from 2016 until now. Figure 3 shows the number of papers that have been published in three different subjects. They are using different security and encryption algorithms in securing cloud computing, securing big data in cloud computing, and using different machine learning algorithms in securing the cloud. It can be noticed from Figure 3 that the number of publications have been increased steadily since 2016 and reached its peak in the last two years 2018 and 2019. Figure 3 indicates that fewer papers have been published in using machine learning algorithms regarding the security of the cloud rather than using different security algorithms for securing the cloud. Further, most of the publications are about securing big data in the cloud with more than 300 publications in a year. In conclusion, more investigations are needed to be conducted using machine learning and security algorithms for securing the cloud.

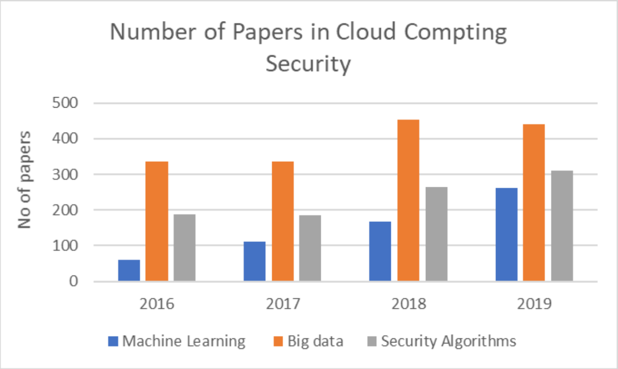

Figure 3. Number of papers in three different subjects since 2016 : "machine learning" represents "using different machine learning algorithms in securing the cloud", "big data" represents "securing big data in the cloud computing ", and "security algorithm" represents "securing the cloud computing"

Figure 4 describes the most commonly used algorithms and methods like Support Vector Machine (SVM), Deep Learning, Neural Network (NN), Naïve Bayes, K-Nearest Neighbors (KNN), and Fuzzy Logic algorithm in securing the cloud in the last year 2019. These ML algorithms have been used in the last years significantly. Based on the analysis of the studies, it can be observed that 43% of papers adopted NN algorithm, 31% deep learning, 13% SVM algorithm, 7% Fuzzy logic, 4% KNN, and only 2% of the papers used Naïve Bayes for securing of the cloud. As a result, the most used algorithms in securing of the cloud are NN, Deep learning algorithms, and SVM, whereas the other algorithms like Fuzzy logic, KNN, and Naïve Bayes have been used less.

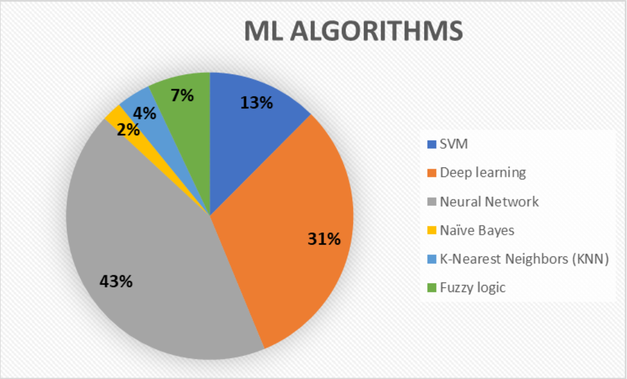

Figure 4. Mostly used ML algorithms in securing the cloud in the year 2019

5. Realted Works

Challenges and threats in a cloud computing system have been explained and pointed in many kinds of research. For example, the work in [2] explained the security challenges in a cloud computing system, different possible solutions, and approaches. The largest cloud service provider (Amazon Web Services or AWS) has been selected as a use case to identify the most important security measures, the infrastructure, and best practices followed by AWS. In [3], many techniques have been identified to protect data that is used by users. The authors explained the issues that affect confidentiality, availability, and integrity of data and proposed some solutions to make the stored data more secure, and confident. Moreover, a survey in [4] classified the challenges and risks in a cloud, into four types in general. The authors defined some solutions and remedies to these risks, and suggested a model for privacy preservation, SLA based security, security overlay network, etc. Similar issues and challenges have been addressed in [5], [6], and [7]. To overcome these challenges and threats, many models and techniques have been proposed and applied. They are summarized and reviewed in the following subsections.

A. Encryption Methods Used for Securing Cloud

Different studies used different encryption algorithms and methods for securing the cloud. For example, Lenka et al. [8] proposed a security model that uses a combination of RSA encryption and digital signature technique which can easily work with all types of cloud computing features. The authors used the RSA encryption algorithm for the confidentiality of data and the MD5 algorithm for authentication. Similar architecture has been proposed in [9] that used AES based file encryption system and asynchronous key system for exchanging data or information. OTP (onetime password) system has been used for user authentication ECC (Elliptic Curve Cryptography) to make the communication between the client and the cloud system safe.

Some works compared the most used encryption algorithms in securing data. The work in [10] compared AES, RSA, Blowfish, and DES algorithms and showed how they are different in case of the platform, key size, scalability, memory usage, encryption time, etc. Also, the work in [11] introduced a mechanism for securing cloud computing and compared the proposed algorithm with some existing algorithms like RSA and AES to prove that the one that has been proposed is more effective.

Other techniques and algorithms have been used to protect the data. As in [12], a model has been proposed using the split algorithm and folder lock to encrypt and decrypt the stored data. In this model, the file is divided into different portions and then stored in different clouds (Multi-cloud Environment). However, a different algorithm has been used to secure the data that is called the KIST algorithm [13]. In this technique, the plain data is converted to cipher data and then transferred on the cloud. When any recovery is needed, the cipher data is converted to plain data then put away on the system.

Some models have been proposed for securing Health care systems. The work in [14] used an e-Health care system as a use case for providing security. The authors proposed an MP-PMDDP (Map-Based Provable Multicopy Dynamic Data Possession) association to avoid document duplicates to question untrusted internet servers. In addition, in [15] a novel system has been proposed for a health care system. The authors used an encryption technique that can perform better than the RSA technique and encrypt every patient's file.

B. Machine Learning for Securing Cloud

Many works have proposed models that use machine learning for securing the cloud environment. For instance, the Artificial Neural Network (ANN) has been used to make the Intrusion Detection System (IDS) more accurate and more stable [16]. The authors used the FC-ANN (Fuzzy-Clustering Artificial Neural Network) to increase the precision and stability of the detection. The same concept has been applied by Ramteke et al. [17] who proposed a system that uses the FC-ANN algorithm. This system automatically records the pattern of the new attack and then stores it in the IDS database. This technique can reduce the human effort and time instead of updating the attack pattern manually.

Machine learning has been used in stenography and image processing for securing data or messages by embedding them into an image or video. Artificial Neural Network (ANN) has been proposed by Kumar et al. [18] for embedding secret messages or extracting messages into or from colored images. A private key embedding algorithm has been used, and the algorithm performance has been analyzed by calculating various parameters like PSNR, MSE. A similar work has been done by Marwan et al. [19]. The authors used Support Vector Machines (SVM) and Fuzzy C-means Clustering (FCM) to classify image pixels more efficiently. As they claimed, SVM can efficiently be used for image segmentation and data protection.

Optimization algorithms have been used for securing the cloud computing system. The works in [20], [21], and [22] used different intelligent algorithms like Particle Swarm Optimization (PSO), Parallel Particle Swarm Optimization (PPSO), Best Fit Decreasing (BFD) algorithm, Genetic Algorithm (GA), Ant Colony Optimization (ACO), etc. These algorithms can be used to optimize the results and utilize the efficiency of the cloud system resources.

Some existing works used machine learning for securing of Mobile Cloud Computing (MCC). In particular, N. Kandavel et al. [23] proposed a Novel Royal Seal Cloudlet (NRSC) for mobile data security and end-to-end mobile-cloud connection. This model is based on a random private token which is used for trusted users. It can provide improved security services, and execution environment, and complete end-to-end security. The work in [24] investigated the possible solutions for mobile cloud computing by using machine learning and the code offloading mechanism. An adaptable Mobile Cloud Computing environment has been developed that is implemented using a cross-platform technology for designing Internet applications. A similar work has been done in [25] .

C. Securing Big Data in Cloud Computing System

Different approaches and algorithms have been used for securing big data. In [26], a model has been proposed which is based on the biological concept of DNA (Deoxyribonucleic Acid) to secure the big data on the cloud. In this method, a 1024-bit secret key is generated based on DNA computing, user's attributes and Media Access Control (MAC) address of the user, DNA bases and complementary rule and decimal encoding rule, and American Standard Code for Information Interchange (ASCII) value. This method enables the system to protect against many security attacks. In addition, a trust aware scheduling solution called Big Trust Scheduling [27] has been proposed that consists of three stages. They are VMs' trust level computation, tasks priority level determination, and trust-aware scheduling.

Many works have studied the efficiency of using the cloud for big data. A distributed approach has been developed with the scalability of partitioning both data and analysis computations into some cloud nodes that can be run independently [28]. In this approach, a framework has been introduced that demonstrates the efficiency of big data, in terms of both analysis performance and accuracy. A Fully Homomorphic Encryption (FHE) has been used as an emerging and powerful cryptosystem that can carry out analytical tasks on encrypted data. In addition, in [29] the efficiency of healthcare big data over cloud computing has been highlighted. The authors discussed many mechanisms with their drawbacks, benefits, and challenges. In addition, an intelligent cryptographic approach has been proposed by Li et al. [30]. In this approach, many algorithms have been used such as Alternative Data Distribution (AD2) Algorithm, Secure Efficient Data Distributions (SED2) Algorithm, and Efficient Data Conflation (EDCon) Algorithm. The proposed model entitled Security-Aware Efficient Distributed Storage (SA-EDS).

Using cloud computing for storing and processing big data has many challenges. The works in [31], [32] , [33], and [34] have discussed and explained the most important issues and challenges. Furthermore, the work in [35] explained how the decision-making process can be improved while using both big data and cloud computing.

6. Comparative Analysis

As we discussed before, many researchers have devoted themselves to study the important issues in securing the cloud. A comparison of such works is illustrated in Table 1 and Table 2.

TABLE 1. ENCRYPTION ALGORITHMS AND METHODS USED FOR SECURING THE CLOUD

		RSA	AES	DES	Blow-fish	OTP	SHA	MD5
Using RSA, AES, and other well-known Algorithms	[8]	✓						✓
	[9]		✓			✓		
Comparing Different Security Algorithms	[10]	✓	✓	✓	✓			
	[11]	✓	✓					
Using other Security Techniques	[12]		✓				✓	
	[13]					✓	✓	
Securing Health-Care Systems	[15]	✓						

Table 1 illustrates some researches that have studied the security of the cloud, using different encryption algorithms and methods. These categories are using RSA, AES, and other well-known Algorithms, comparing different security algorithms, using other security techniques, and securing Health-Care systems.

Many studies used different encryption algorithms. As Table 1 shows, some studies used well-known encryption algorithms like AES, DES, and RSA for data encryption [8]- [12]. Some of them used a combination of encryption algorithms with authentication techniques such as MD5, OTP, or SHA-1 [8], [9], [12], [13]. Moreover, a novel system has been proposed that uses an improved RSA technique to encrypt every patient's file [15].

Machine learning is one of the most popular research fields. Many studies have addressed the security of the cloud using different ML algorithms. Table 2 shows different categories of studies that have been conducted for securing the cloud using ML.

TABLE 2. MACHINE LEARNING ALGORITHMS USED FOR CLOUD COMPUTING SECURITY

		ANN	SVM	Regression	GA	PPS	Clustering K-means	Fuzzy C-means Clustering
Using Clustering and ANN	[16]	✓						✓
	[17]	✓						✓
ML used in Stenography and Image processing	[18]	✓						
	[19]		✓					✓
	[36]		✓					
Using optimization algorithms	[20]				✓	✓		
	[21]	✓		✓		✓		
	[22]			✓				
Using clustering	[37]						✓	
	[38]						✓	

Researchers used different ML algorithms and techniques in securing the cloud. As Table 2 shows, some studies used Artificial Neural Network (ANN) algorithm to secure the cloud [16] [17] [18] [21], whereas other studies used SVM (Support Vector Machine) to secure the data on the cloud [19] [36]. In addition, some researchers used a regression algorithm for the security of the cloud [21] [22]. Moreover, some used optimization techniques in machine learning such as the Genetic Algorithm (GA) and Parallel Particle Swarm (PPS) algorithm [20] [21]. [37] and [38] used the Clustering K-means algorithm to secure the cloud computing system. In addition, some works used Fuzzy C-means Clustering to improve the precision and efficiency in the provided results [16], [17], [19].

7. Cloud Security Challenges

Security is an important issue in a cloud computing paradigm that affects the adoption of cloud computing technology. Providers of a cloud are responsible for employing and applying different security mechanisms, in order to make sure that the data and applications are secured. Data phishing, data loss, downtime, password weakness, data disclosure, and other threats that are related to network, security, and applications are still occurring in many companies. These security issues and challenges lead to a decrease in the acceptance of cloud computing technology.

Like other security systems, the cloud computing paradigm suffers from many issues and challenges. There are many security challenges that depend on different deployment methods in the cloud. One of the major challenges is the privacy issue. In a cloud paradigm, the privacy issue depends on the cloud deployment model. For example, in a public cloud, access is through the Internet, and data can be used by a broad number of users. In this case possibility of data loss or data disclosure is more. In a SaaS environment, the user data is on the cloud and the control over the application is in the hand of the provider. Therefore, there is a risk of data disclosure and exploitation. There are many issues and problems related to virtualization and network. Many studies have addressed the main problems and challenges in securing the cloud. To increase the trust between the user and the cloud provider and provide the users with an accurate and secured cloud system, more sophisticated solutions and up-to-date mechanisms should be provided.

Security issues and challenges can be reviewed from different perspectives. They can be divided into security issues that are related to data centers, virtualization, and networks. The following subsections explain the security issues and challenges for each.

A. SECURITY ISSUES RELATED TO DATA CENTERS

One of the issues related to data centers is the service provider that performs the services. The user of the cloud must ensure that the cloud service provider is performing the cloud services correctly upon the agreements that have been done between the user and Cloud Service Provider (CSP). This is to ensure protection from attacks at different levels. There should be a technique to ensure the quality of services in terms of attack, encryption algorithms, and authentication methods that have been used. All can be defined by using XML and SOAP messages, and SSL (Secure Sockets Layer) with transport layer security.

In a cloud paradigm, it is very important to make sure that the user's private data is separated from other users. If the data for the users is to be in one shared environment, the data will be vulnerable to attacks. In this case, the viruses can be spread from one user to another, and affect the integrity and the availability of data. To avoid such cases, the cloud service provider must ensure that the user private data is separated from others and is secured.

To ensure a storage location for the cloud user, it might be very difficult for a service provider because of limitations and restrictions on techniques. The cloud user's data is stored automatically on the data centers that are provided everywhere unless the service provider uses dedicated servers for dedicated users. This is because of the restrictions on techniques and logistics provided in a cloud computing paradigm. Requesting, processing, and storing of data usually are done in different places.

The existence of data on a third-party device is another issue that should be considered. In this case, the data is vulnerable to attacks as user private data exists in others' computers. To avoid this problem, private data should exist only in secured places, and the locations of data should be organized in a way so that the user knows where the data is hosted.

B. SECURITY ISSUES RELATED TO VIRTUALIZATION

Virtualization is an essential part of any cloud computing paradigm. There are many issues that should be considered when using virtualization. It is very common that a VM hypervisor is vulnerable to an attack and be compromised. To avoid such cases, a powerful security monitoring application should exist.

Another concern with virtualization is allocating and deallocating resources with VMs. Data are written into physical memory when VMs are operating. If the data is not deleted before the resources are reallocated to other VM, there is a possibility that the data will be compromised. Not all operating systems manage the data clearing. Consequently, the user should make sure that a released resource was cleared and cleaned. Further, the traffic flow between VMs should be managed. VLANs are used to isolate the traffic among user's virtual machines.

C. SECURITY ISSUES RELATED TO NETWORK

The network is a backbone for any cloud computing system. Many issues and challenges should be considered and encountered while using the network in a cloud paradigm. Cloud users should be able to identify bandwidth requirements for the hosted application in the cloud. Insufficient bandwidth among servers will lead to a significant latency beyond acceptable limits in a Service Level Agreement (SLA) for the hosted applications.

In many companies, different applications and software are installed to avoid attacks and malicious codes. Examples of these applications are Intrusion Detection Systems (IDSs), and firewalls. It is important to make sure that other applications are adaptable with these security applications. Furthermore, servers and other network devices are related to the network. Therefore, they cannot easily be migrated from one network to another because a network device like a server is defined according to the VLAN that it belongs to. As a result, to increase resource flexibility and utilization, network policies should be applied.

In some cases, enterprises need to use services that exist on multiple clouds and are managed by different Cloud Service Providers (CSPs). In these cases, cloud interoperability, and the ability to share different types of information becomes mandatory. Connectivity among the data centers should be provided, to make all data centers as one cloud within the control of CSPs.

8. Future Directions

The stored data in a cloud is not fully secured. Many attacks and malicious codes exist on the Internet. These attacks try to steal or destroy the private data and systems in the cloud. Small companies that are using the cloud may have not provided good security practices. To avoid cyber-attacks, good security measurements are required that should be applied by cloud providers.

Many researchers have studied the security of the cloud and proposed different models and technologies, to reach to a security level that satisfies the cloud user and the cloud provider. They have studied in different areas in the security and tried many models with different techniques and tools to overcome the shortages and challenges that they are facing.

To increase the level of security in the cloud, we need to consider existing issues and challenges, the countermeasures, and possible solutions to the challenges. As technology improves year by year, more sophisticated solutions are needed to overcome these challenges. Consequently, more efficient and sophisticated models should be designed that address issues like visualization in a cloud computing system, compromised services, data compatibility among different cloud providers, and regulatory compliances. Moreover, the solutions provided in different structures of a cloud such as Paas and Iaas should be expanded for public and private sectors. The amount of storage for the cloud should be increased for different companies and individuals. The quality of the Internet should be improved to make sure that the cloud is performing without any interruption or downtime. As a result, cloud computing services will be delivered to the users with the best quality.

9. Conclusions

As the cloud computing system becomes a dominant technology nowadays, it is very important to build trust between the users and the cloud providers. Consequently, cloud computing security has become a general concern for the researchers who are working with the cloud paradigm. Moreover, many studies and researches have been conducted with new methods and techniques to make the cloud security more powerful and sophisticated. In addition, many studies have been done to overcome the existing challenges and issues related to cloud security. In this paper, a literature review of different studies has been done from different perspectives. Further, a taxonomy and an analysis of the previous works have been shown and discussed to provide a complete and comprehensive vision of existing techniques and methods. In addition, the security issues and challenges in a cloud computing system have been addressed to provide general information about the existing shortfalls and gaps in the security of the cloud. Consequently, future directions have been discussed to let the researchers make further researches and studies to overcome the security issues and challenges.

References

[1] M. T. Tapale, M. N. Birje, P. S. Challagidad, and R. H. Goudar, “Cloud computing review: concepts, technology, challenges and security,” Int. J. Cloud Comput., vol. 6, no. 1, p. 32, 2017, doi: 10.1504/ijcc.2017.10004732.

[2] F. Shahzad, “State-of-the-art survey on cloud computing security challenges, approaches and solutions,” Procedia Comput. Sci., vol. 37, pp. 357–362, 2014, doi: 10.1016/j.procs.2014.08.053.

[3] S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, 2016, doi: 10.14569/ijacsa.2016.070464.

[4] A. Garg and R. Rathi, “A Survey on Cloud Computing Risks and Remedies,” Int. J. Comput. Appl., vol. 178, no. 29, pp. 35–37, 2019, doi: 10.5120/ijca2019919139.

[5] N. H. Hussein and A. Khalid, “A survey of cloud computing security challenges and solutions,” Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 1, pp. 52–56, 2016, [Online]. Available: http://search.proquest.com.library.capella.edu/docview/1764183503?accountid=27965%5Cnhttp://wv9lq5ld3p.search.serialssolutions.com.library.capella.edu/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ:criminaljusticeperiodicalsshell&rft.

[6] N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” Comput. Electr. Eng., vol. 71, no. June, pp. 28–42, 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[7] R. Velumadhava Rao and K. Selvamani, “Data security challenges and its solutions in cloud computing,” Procedia Comput. Sci., vol. 48, no. C, pp. 204–209, 2015, doi: 10.1016/j.procs.2015.04.171.

[8] S. R. Lenka and B. Nayak, “Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm,” vol. 2, no. 3, pp. 60–64, 2014.

[9] A. Hussain, C. Xu, and M. Ali, “Security of Cloud Storage System using Various Cryptographic Techniques,” Int. J. Math. Trends Technol., vol. 60, no. 1, pp. 45–51, 2018, doi: 10.14445/22315373/ijmtt-v60p509.

[10] R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," Int. J. Eng. Res. Appl., vol. 3, no. 4, pp. 1922–1926, 2013.

[11] T. Bharathan and B. J. Santhosh Kumar, "Implementing information security mechanism over cloud network," Int. J. Recent Technol. Eng., vol. 8, no. 2, pp. 1706–1710, 2019, doi: 10.35940/ijrte.B1033.078219.

[12] S. Sharma, "Enhancing Data Security Using Encryption and Splitting Technique over Multi-Cloud Environment," vol. 5, no. 3, pp. 1041–1047, 2019, [Online]. Available: https://ijsret.com/wp-content/uploads/2019/05/IJSRET_V5_issue3_321.pdf.

[13] A. V. Bhabad, "Data Confidentiality and Security in Cloud Computing Using KIST Algorithm," Int. J. Emerg. Trends Sci. Technol., pp. 3831–3837, 2016, doi: 10.18535/ijetst/v3i05.02.

[14] K. Vijaya Swetha, P. Sai Kiran, and K. V. V. Satyanarayana, "Privacy and Auditability in Cloud Assisted Health Data," Asian J. Inf. Technol., vol. 18, no. 4, pp. 133–138, 2019, doi: 10.36478/ajit.2019.133.138.

[15] K. Sharma, A. Agrawal, D. Pandey, R. A. Khan, and S. K. Dinkar, "RSA based encryption approach for preserving confidentiality of big data," J. King Saud Univ. - Comput. Inf. Sci., no. xxxx, 2019, doi: 10.1016/j.jksuci.2019.10.006.

[16] G. K. Chaturvedi, A. K. Chaturvedi, and V. R. More, "A study of intrusion detection system for cloud network using FC-ANN algorithm," vol. 4, no. 3, pp. 482–487, 2016, [Online]. Available: https://pdfs.semanticscholar.org/1b65/42ee7e5e3855ea9682d165eb893fde22b354.pdf.

[17] S. Ramteke, R. Dongare, and K. Ramteke, "Intrusion Detection System for Cloud Network Using FC-ANN Algorithm," Int. J. Adv. Res. Comput. Commun. Eng., vol. 2, no. 4, pp. 1818–1822, 2013, [Online]. Available: www.ijarcce.com.

[18] "A SECURE STEGANOGRAPHY APPROACH FOR CLOUD DATA USING ANN ALONG WITH," vol. 16, no. 6, pp. 86–92, 2018.

[19] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," Procedia Comput. Sci., vol. 127, pp. 388–397, 2018, doi: 10.1016/j.procs.2018.01.136.

[20] N. K. Gondhi and A. Gupta, "Survey on Machine Learning based scheduling in Cloud Computing," ACM Int. Conf. Proceeding Ser., vol. Part F1278, pp. 57–61, 2017, doi: 10.1145/3059336.3059352.

[21] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," Meas. J. Int. Meas. Confed., vol. 119, no. July 2017, pp. 117–128, 2018, doi: 10.1016/j.measurement.2018.01.022.

[22] S. Mashhadi Moghaddam, M. O'Sullivan, C. Walker, S. Fotuhi Piraghaj, and C. P. Unsworth, "Embedding individualized machine learning prediction models for energy efficient VM consolidation within Cloud data centers," Futur. Gener. Comput. Syst., vol. 106, pp. 221–233, 2020, doi: 10.1016/j.future.2020.01.008.

[23] N. Kandavel and A. Kumaravel, "A Novel Royal Seal Cloudlet for Security Enhancement in Mobile Cloud Computing," Int. J. Comput. Sci. Inf. Secur., vol. 17, no. 1, pp. 1–7, 2019, [Online]. Available: https://sites.google.com/site/ijcsis/.

[24] P. Nawrocki, B. Sniezynski, and H. Slojewski, "Adaptable mobile cloud computing environment with code transfer based on machine learning," Pervasive Mob. Comput., vol. 57, pp. 49–63, 2019, doi: 10.1016/j.pmcj.2019.05.001.

[25] S. Dey, Q. Ye, and S. Sampalli, "A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks," Inf. Fusion, vol. 49, no. December 2018, pp. 205–215, 2019, doi: 10.1016/j.inffus.2019.01.002.

[26] S. Namasudra, D. Devi, S. Kadry, R. Sundarasekar, and A. Shanthini, "Towards DNA based data security in the cloud computing environment," Comput. Commun., vol. 151, no. October 2019, pp. 539–547, 2020, doi: 10.1016/j.comcom.2019.12.041.

[27] G. Rjoub, J. Bentahar, and O. A. Wahab, "BigTrustScheduling: Trust-aware big data task scheduling approach in cloud computing environments," Futur. Gener. Comput. Syst., no. xxxx, 2019, doi: 10.1016/j.future.2019.11.019.

[28] A. Alabdulatif, I. Khalil, and X. Yi, "Towards secure big data analytic for cloud-enabled applications with fully homomorphic encryption," J. Parallel Distrib. Comput., vol. 137, pp. 192–204, 2020, doi: 10.1016/j.jpdc.2019.10.008.

[29] L. Rajabion, A. A. Shaltooki, M. Taghikhah, A. Ghasemi, and A. Badfar, "Healthcare big data processing mechanisms: The role of cloud computing," Int. J. Inf. Manage., vol. 49, no. April, pp. 271–289, 2019, doi: 10.1016/j.ijinfomgt.2019.05.017.

[30] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Inf. Sci. (Ny)., vol. 387, pp. 103–115, 2017, doi: 10.1016/j.ins.2016.09.005.

[31] A. Kobusińska, C. Leung, C. H. Hsu, S. Raghavendra, and V. Chang, "Emerging trends, issues and challenges in Internet of Things, Big Data and cloud computing," Futur. Gener. Comput. Syst., vol. 87, pp. 416–419, 2018, doi: 10.1016/j.future.2018.05.021.

[32] C. Yang, M. Yu, F. Hu, Y. Jiang, and Y. Li, "Utilizing Cloud Computing to address big geospatial data challenges," Comput. Environ. Urban Syst., vol. 61, pp. 120–128, 2017, doi: 10.1016/j.compenvurbsys.2016.10.010.

[33] N. M. Elzein, M. A. Majid, I. A. T. Hashem, I. Yaqoob, F. A. Alaba, and M. Imran, "Managing big RDF data in clouds: Challenges, opportunities, and solutions," Sustain. Cities Soc., vol. 39, no. February, pp. 375–386, 2018, doi: 10.1016/j.scs.2018.02.019.

[34] L. Zhou, A. Fu, S. Yu, M. Su, and B. Kuang, "Data integrity verification of the outsourced big data in the cloud environment: A survey," J. Netw. Comput. Appl., vol. 122, no. April, pp. 1–15, 2018, doi: 10.1016/j.jnca.2018.08.003.

[35] B. M. Balachandran and S. Prasad, "Challenges and Benefits of Deploying Big Data Analytics in the Cloud for Business Intelligence," Procedia Comput. Sci., vol. 112, pp. 1112–1122, 2017, doi: 10.1016/j.procs.2017.08.138.

[36] A. Sukumar, V. Subramaniyaswamy, V. Vijayakumar, and L. Ravi, "A secure multimedia steganography scheme using hybrid transform and support vector machine for cloud-based storage," Multimed. Tools Appl., 2020, doi: 10.1007/s11042-019-08476-2.

[37] Q. yu Zhang, Z. xian Ge, Y. jie Hu, J. Bai, and Y. bo Huang, "An encrypted speech retrieval algorithm based on Chirp-Z transform and perceptual hashing second feature extraction," Multimed. Tools Appl., vol. 79, no. 9–10, pp. 6337–6361, 2020, doi: 10.1007/s11042-019-08450-y.

[38] S. Sandosh, V. Govindasamy, and G. Akila, "Enhanced intrusion detection system via agent clustering and classification based on outlier detection," Peer-to-Peer Netw. Appl., 2020, doi: 10.1007/s12083-019-00822-3.

Zainab Salman is a Lab Instructor working at University of Bahrain. She is currently studying Ph.D. in University of Bahrain in Computing and Information Sciences. She received her Master's degree in Computer Science from Al Ahlia University, Bahrain in 2010 and her B.Sc. in Computer Science from University of Bahrain in 2005. Her research interests include cloud computing and security.

Mustafa Hammad is an Associate Professor in the Department of Computer Science at the University of Bahrain. He received his Ph.D. in Computer Science from New Mexico State University, USA in 2010. He received his Master's degree in Computer Science from Al-Balqa Applied University, Jordan in 2005 and his B.Sc. in Computer Science from The Hashemite University,Jordan in 2002. His research interests include machine learning, software engineering with focus on software analysis and evolution.