Hindawi
Scientific Programming
Volume 2020, Article ID 8871315, 31 pages
https://doi.org/10.1155/2020/8871315

Review Article

Security Measurement in Industrial IoT with Cloud Computing Perspective: Taxonomy, Issues, and Future Directions

Sahar Shah,[1] Mahnoor Khan,[2] Ahmad Almogren,[3] Ihsan Ali,[4] Lianwen Deng,[5] Heng Luo,[5] and Muazzam A. Khan[6]

[1]*Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan*
[2]*Department of Physics, Government Post Graduate College, Nowshera, Pakistan*
[3]*Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia*
[4]*Faculty of Computer Science and IT, University of Malaya, Kuala Lampur, Malaysia*
[5]*School of Physics and Electronics, Central South University, Changsha, China*
[6]*Department of Computer Sciences, Quaid-i-Azam University, Islamabad, Pakistan*

Correspondence should be addressed to Ahmad Almogren; ahalmogren@ksu.edu.sa and Ihsan Ali; ihsanalichd@siswa.um.edu.my

Received 6 September 2020; Revised 4 October 2020; Accepted 8 October 2020; Published 26 October 2020

Academic Editor: Shah Nazir

In recent years, cloud computing has gained massive popularity in information technology and the industrial Internet of things. It provides facilities to the users over the wireless channel. Many surveys have been carried out in cloud security and privacy. The existing survey papers do not specify the classifications on the basis of cloud computing components. Therefore, they fail to provide the techniques with their specialities as well as the previously available literature review is outdated. This paper presents the security for cloud computing models with a new aspect. Unlike the previously existing surveys, the literature review of this paper includes the latest research papers in the field of cloud security. Also, different classifications are made for cloud computing security on the basis of different cloud components that are used to secure the cloud models. Furthermore, a total of eleven (11) classifications are considered, which includes cloud components to secure the cloud systems. These classifications help the researchers to find out the desired technique used in a specific component to secure the cloud model. Moreover, the shortcoming of each component enables the researchers to design an optimal algorithm. Finally, future directions are given to highlight future research challenges that give paths to researchers.

1. Introduction

This survey paper is organized in such a manner in which Section 1 contains an introduction to cloud computing, applications, and security. Section 1.1 is the contribution of our survey paper to the field of cloud computing security. Section 2 is called the literature review. The whole literature review section is subdivided into eleven (11) classification components. Every classification includes different research articles and at the end of each classification component a table is drawn which summarizes the overall classification component. After Section 2, the next is Section 3, the conclusion section, which concludes the presented survey. Then, in Section 4 the future research directions are discussed. At last, all the acronyms used in this manuscript are listed in Table 1. Figure 1. shows the organization of the manuscript.

The word cloud is described in 2006 for the business models which provide services over the Internet and the availability of data is the main concern in cloud storage [1]. According to NIST, cloud computing is classified into two major categories. One is based on services and the other is based on deployment models [2]. The service cloud computing category is further classified into three types: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). The deployment category

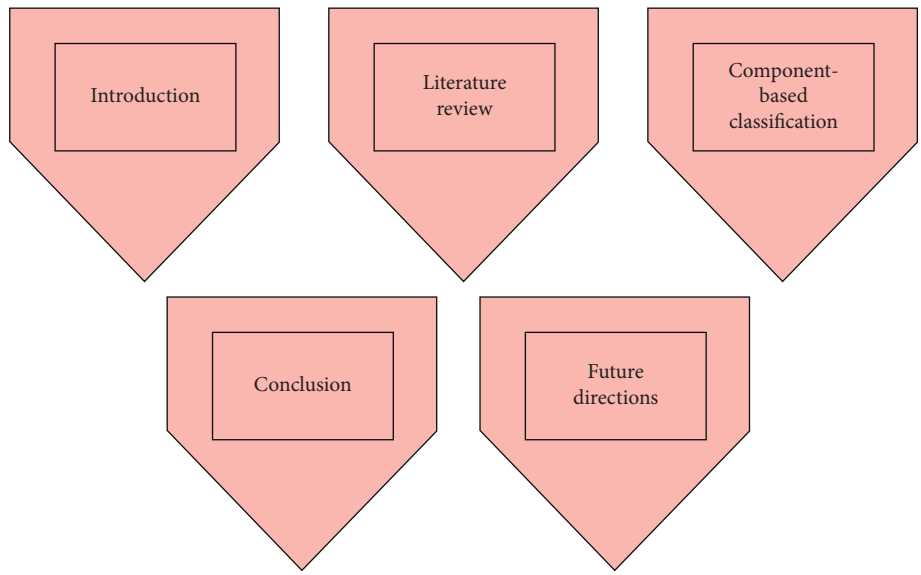

Figure 1: Organization of the manuscript.

is classified into the public cloud (P_b), private cloud (Pr_C), hybrid cloud (HC), and community cloud (CC). In the SaaS model, the overall software services are offered on the cloud. In the PaaS model, the development platforms are offered on the cloud. In the IaaS model, all the services related to hardware in a cloud are performed. While, in the P_bC type of cloud related to a specific organization and not connected to any other firm, such clouds have high costs and security. In P_rC type, the infrastructure is hosted by the traders of the cloud. The user has no control in this framework. The combination of P_bC and P_rC is called HC which is a scalable and cost-effective cloud. Mobile computing is used to encounter the security challenges in IoT [3]. In the CC model, infrastructure is shared between several organizations from a specific community. Furthermore, NIST also describes the most extremely important parameters. These parameters differentiate the cloud computing from the others, namely, on-demand self-service, broad network access, resource pooling, rapid elasticity, and measurement service.

The cloud computing field took huge attention of the researchers in information technology by having different powerful parameters. The parameters cost reduction, on-demand self-service, rapid elasticity, resource pooling, broad network access, high service scalability, flexibility, and high capacity of storage to afford the big data [4]. Many problems in the business domain have been solved by cloud computing and provide an efficient platform for the business community. These all advantages switched the many business communities to put their IT infrastructure to a cloud environment.

Obviously, cloud security and privacy are important parameters in every cloud system. If no proper security and privacy are provided to cloud models, then the cloud models will be no longer used. Cloud security and privacy are major barriers to cloud service adoption. The cloud security parameters attract the noncloud models toward the cloud framework. To provide security to the cloud computing components, different techniques are applied. The cloud security is responsible to provide a leakage-free, hijacker-free, and threat-free cloud system. The cloud environment is widely shared and aggressive [5]; hence, different blitz at a cloud network, framework, and approach to cloud duty can affect both the accessibility and security of the cloud computing. These risks and blitz can be inside and outside cloud. Inner risks and blitz are further classified into two divisions: one is malevolent insider working and the other is working inside for an organization. Fog-based IoT healthcare has an optimal response in terms of energy consumption and network delay of the fog nodes [6]. The cloud computing environment is distributed among companies and users. Therefore, cloud service distributors should maintain several basic mechanisms to strengthen cloud services in the security aspect. The industrial IoT merged the representative technologies such as machine-machine communication and 5G [7].

Many research articles, regarding cloud security and privacy, have been published. In [8], cloud security is classified into five different categories. The classification in this article is on the basis of security basics, structure, access control, cloud framework, and data. Numerous devices can be connected to IoT for industrial applications [9]. The basic analysis scheme called the Service Measurement Index (SMI) is developed in [10] for the industrial Internet of things. The SMI is further classified into seven subdivisions and one of them is cloud security. The subdivision of cloud security includes Access Control and Privilege Management, Information Privacy, and Loss. The industrial IoT is used for business purpose in China this business is in three aspects resources efficiency, sustainable energy, and transparency [11].

In this survey, cloud security and privacy are analyzed in a different aspect. Different techniques, tools, software, and algorithms are used in cloud components to strengthen the cloud system. This paper classifies cloud computing into eleven (11) categories, as shown in Figure 2. The

classifications involve different cloud components in which different methods, techniques, policies, models, approaches, software, and tools are used to enhance cloud security and privacy. Every classification is further subdivided into the overviews, advantages, the techniques used, and the paper publication year. This work provides the easiest way to the researchers in finding where, when, and how to use a cloud component for security purposes in any cloud model. The demerits of each classification provide an opportunity for scientists and researchers to design an efficient technique. Then, in future trends, all the deficiencies related to the specific cloud computing component observed can be enhanced and modified further.

1.1. Our Contributions. Shortly, the paper contributes in the following ways:

(i) This survey considers the classifications, based on different techniques used in cloud computing components, to secure the cloud model. The paper classifies the literature review into eleven (11) different classifications used to make sure the cloud security. Each classification includes various articles. The table is provided with each classification in which the overview, advantages, techniques, references, and the years are mentioned. This approach makes the easiest way for the researchers to find out the concerned cloud component related to any specific security issue in cloud computing. While the other surveys do not classify the cloud computing security into different classifications, which is a struggle for the researchers in finding the technique used, its advantages, and demerits.

(ii) Many survey articles in cloud computing security have been published. The shortcoming exists in their work. They include the oldest papers in the literature review, while, in this survey, the latest papers were included from 2015 to 2020 in the literature review section.

(iii) In this survey, all the possible future directions in cloud security are mentioned. The techniques, software, etc. used in cloud computing components have different flaws. This paper addresses them which helps to enhance them in future work. However, previously published surveys fail to discuss these flaws. Table 2 shows the differentiation key points which differentiate our survey from the existing surveys.

(iv) The bibliographic-based survey performed in our paper while the other surveys fail to do this. This bibliographic-based survey involved country-, author-, and year-based surveys in the field of cloud computing security. This shows the top authors, countries, and years which have the main role in cloud computing security.

(v) Due to the high demand for cloud computing models, the cloud setup enhances its storage capacity at low cost. Cloud models increase the number of tools and machine learning functions. These enforced the organizations to move on a cloud computing-based platform. Besides these points, the advancement of the cloud computing model from earlier is based on five points. (i) Earlier, from two decades, the cloud computing models more clarify and simplify the customer touch-points. (ii) Creating a definition of Internet protocol (IP) ownership related to artificial intelligence (AI). (iii) Minimizing risk and simplifying multicloud. (iv) Creating a more robust sales and partner strategy. (v) Delivering platform innovation.

Table 2 is for the sake of simplicity, which differentiates this survey from the already existing surveys on the basis of key parameters. The tick symbol shows the inclusion of the parameters such as parametric-based survey, contribution section, cloud security applications, component-based classifications, and future trends in the respective survey, while the cross symbol shows the parameters not included in the mentioned survey papers.

2. Literature Review

2.1. Classifications. The literature review section is divided into different classifications according to cloud computing components used to secure the cloud systems. Table 3 illustrated different classified components which are categorized for the cloud security purposes and contains different number of articles. Figure 3 shows the classification of the related work in the form of bar graph which includes number of years versus number of papers.

2.2. Storage-as-a-Service. Table 4 shows the references, overviews, algorithms, techniques used, and advantages along with the publication years for each paper included in this category of the classification. Data security needs serious attention as the cloud storage increases day by day. In [20], the cloud storage security policy is analyzed. The model permits the users to avail of the resources on-demand including computer and storage systems providing fast, efficient, and inexpensive computing. Such a specification of a cloud model makes it a large data cloud computing model from the tradition cloud model. There is no standardization, normalization, security policy, and security mechanism in the process of data transmission of cloud storage technology. In the network layer, data is not only leaked in the form of electromagnetic waves but also intercepted in network communication. So, by this the hackers can take advantage of vulnerabilities and technical errors of the network. By using the technology in an improper way, the data in the data link, network, and transport layers will be at risk; even SSL, SSH, IPSEC, and other VPN technologies are considered. The cloud storage system is a complex method and needs the security arrangements of different cloud providers have their security policies and technical solutions. However, there are two types of risk on data storage called hardware application strategy and cloud storage service providers management.,

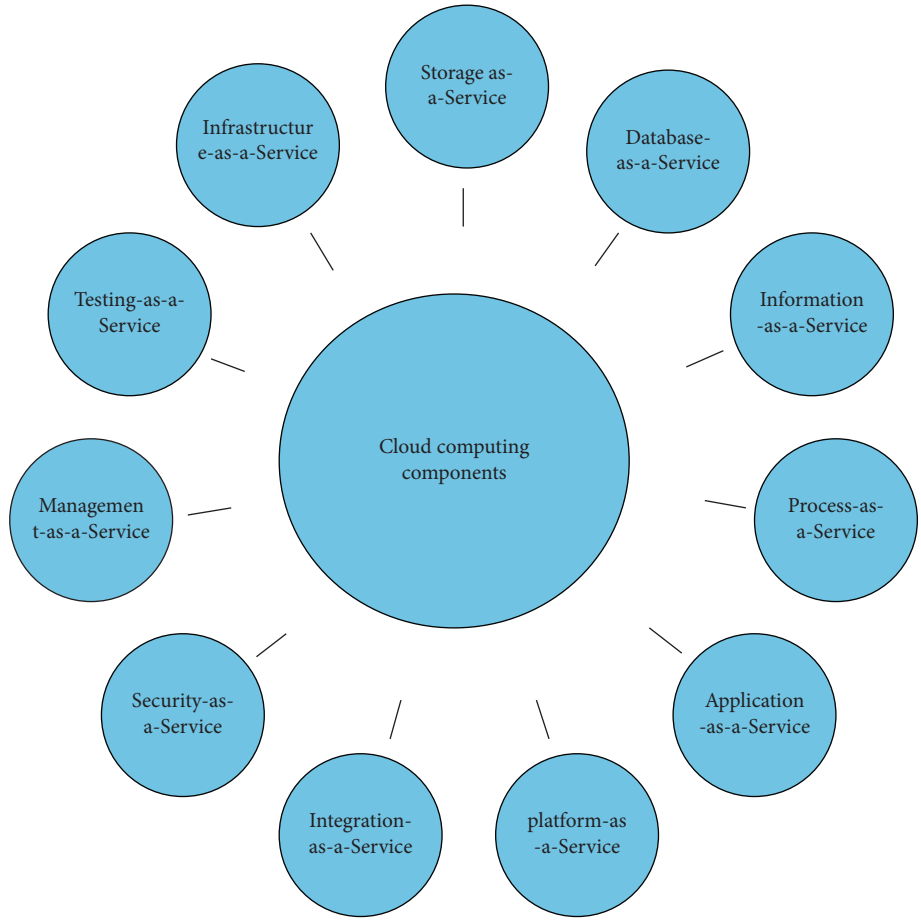

Figure 2: Cloud component-based classification.

In this framework, the online distributed storage system is presented, in which the identity authentication, access control, and encrypt transmission techniques are used to protect the cloud storage system from the security threats. In this model, firstly, confirmation of user identity has been done to create mutual authentication among the user and cloud storage server. Secondly, to protect data from threats, the end-to-end data transmission is achieved using encryption on it. Thirdly, to ensure that the data is not used by any other unauthentic person, access control is used. These all protect the data regarding integrity, availability, and confidentiality. The encryption method provides the confidentiality of the data. The data is fragmented in this model using Shamir's threshold secret sharing program. The data storage security assurance is obtained by using data scattered storage technology, and there is a direct relationship between the error rate of storage data and storage system capacity. The data store in the cloud storage model, and then it is distributed in different places through which distributed online cloud storage security is achieved. In short, in this model, some technical issues regarding security are discussed on layers and data storage cloud, which gives their protecting solutions.

In [21], the addressing of the data placement problem in a cloud system is proposed. To overcome the problem of high data retrieval time and threat level for data security, an intelligent method that achieves high performance along with the security satisfaction is discussed in the proposed framework. In this work, a novel approach that addresses the data placement in a cloud storage system is discussed. The whole work is divided into steps. In the first step, the linear data programming model is formulated for the data placement problem. This is responsible for reducing the data retrieval time and distributing over different storage nodes. In the second step, a heuristic algorithm called the SADP mechanism developed to solve the problem for the cloud storage system (Sedulous). Therefore, a novel approach is needed which guarantees data security by minimizing the overhead of the security service. The performance issue with the security requirement creates the problem of data placement. To solve this issue the entire data file is divided into multiple numbers and the data spread over the pieces of the file and each will store in a separate mode. These pieces of the file spread over storage nodes with a specific distance between any two pairs of the fragments. This mechanism ensures that if an attacker successfully enters a piece of file data, then it is unable to leak, reveal, and find the location of the meaningful data of the user. By solving the three subproblems, the data placement issue can be solved. The three problems are the decision of the number of chunks, the decision of the size of each chunk, and, the last but not the least, the selection of storage nodes. These three issues are

Table 1: Abbreviation used in the paper.

Abbreviations	Words
PaaS	Platform-as-a-service
SaaS	Software-as-a-service
IaaS	Infrastructure-as-a-service
Pb	Public cloud
Pr	Private cloud
HC	Hybrid cloud
NE	Nash equilibrium
CSU (s)	Cloud service user (s)
CSP (s)	Cloud service provider (s)
CI	Cloud infrastructure
SSG	Security Stackleberg game
FEBM	Feedback evaluation and Bayesian model
CSPM	Cloud security and privacy model
NIST	National Institute of Standards and Technology
ACPML	Access control and privilege management layer
CCAF	Cloud computing adoption framework
BPMN	Business process modeling Notation
CISL	Cloud infrastructure security layer
PESL	Physical environmental security layer
HTTP	Hypertext transfer protocol
DDoS	Distributed denial of service
SDLC	Software development life cycle
ABDS	Attribute-based data sharing
DAC	Data access control
SK (s)	Secret key (s)
PSSFP	Previous-selected-server-first policy
MOO	Multiobjective optimization
DFS	Distributed file system
CCTV	Closed circuit television
IM-SecaaS	Intrusion management Security-as-a-Service
OPEX	Operational expense model
IDPS	Intrusion detection/prevention system
CEPM	Compliance enforcement and policy management
SSDP	Simulation software development process
ADIRS	Attack detection and intrusion rejection system
CSA	Cloud security Alliance
SecSLA	Security service level agreement
QPT	Quantitative policy trees
QHP	Quantitative hierarchical process
QoS	Quality of service
DoS	Denial of service
PM	Privacy manager
GA	Genetic algorithm
SADP	Security-aware data placement
PSO	Particle Swarm optimization
ACO	Ant colony optimization
CAS	Chaotic ant Swarm
GA-CAS	Genetic algorithm-based chaotic ant Swarm
MHA (s)	Metaheuristic algorithms
NDTMSI	Nondeterministic task meta-Schedular integrated
AES	Advanced encryption standard
HEVC	High efficiency video coding
IEVS	Intraencoded video stream
TLS	Transport layer security
SED2	Secure efficient data distribution
EDcon	Efficient data conflation
MDMCO	Multidimensional and multiconstraint optimization
BC (s)	Blockchain (s)
BPDPP	Blockchain's public and distributed peer-to-peer
BWH	Block withholding
PoW	Proof-of-Work
PPLN	Pay-per-Last N
SBOS	Security benchmark for open stack
PKE	Public key encryption
SLA (s)	Service level agreement (s)

solved by introducing a linear programming model, a fast heuristic algorithm called Sedulous. The Sedulous follows a greedy approach in which the preference is given to the nodes which can transmit data with high speed. For the security addressing, the T-coloring approach used makes sure that the two adjacent nodes will never be with the same colors, in which they never store the simultaneous chunks of data. The simulation results show that the presented framework reduces the retrieval time up to 20 percent for the random network topology and 19 percent for the Internet topology systems, and these results were compared with the baseline methods and only the security parameter was noticed. The results also show that the model achieves minimum retrieval with the best performance and data security. However, the proposed work scarifies the rejection ratio and reduces the cost of the commercial cloud provided.

The huge data can be stored on cloud storage with no limitation of storing memory. In [22], to secure the cloud data in an open platform, an efficient scheme is proposed. The scheme encrypts and decrypts the files of data, multiple auditing processes, and uses dynamic operations with the integrity of data. From start to end, the whole algorithm is divided as the start, public audibility of data files, checking data dynamics, verifying integrity proof, multiple batch auditing processes, privacy-preserving public auditing scheme, process storage system, and end.

In [23], the authors target different security issues that cannot be ignored and which degrade the performance and trust of the CSPs. The proposed work then evaluates the security issues of the cloud by proposing techniques to make sure the security of the cloud. Different issues in the cloud are data loss or leakage, account, insecure interfaces, dos, and abuse and nefarious use. The article focuses to store the data in the cloud with strong security. To store the data in the cloud, it is first divided into small and large pieces and then put on the different media. Every small and large piece of data has its advantages and disadvantages, i.e., the large piece of data is easy to follow and read while the small piece is difficult in terms of detrimental performance. The hackers can hijack and target large piece of data because it is easy to follow and read. The proposed framework encrypts the piece of data through programming before putting them on the different media and decrypts it gain on the user side. The symmetric encryption, also called a public key cryptographic approach, is applied to the data to encrypt it due to the larger size of data. The symmetric encryption approach is preferred rather than the asymmetric approach due to the public key algorithm and to encrypt big data files especially in

Table 2: Key points which differentiate our survey from the existing surveys.

References	Years of publication	Parametric-based survey	Contributions	Cloud security applications	Component-based classifications	Future trends
[12]	2017	x	x	x	X	x
[13]	2018	x	x	x	X	x
[14]	2018	x	x	x	x	x
[15]	2015	x	x	x	x	x
[16]	2016	x	x	x	x	x
[17]	2020	x	x	x	x	x
[18]	2020	x	x	x	x	x
[19]	2019	x	x	x	x	x
Our survey		√	√	√	√	√

Table 3: Number of papers in each classification.

Sections	Classification title	Number of papers	References
2.2	Storage-as-a-Service	Seven	[20–26]
2.3	Database-as-a-Service	Three	[5, 27, 28]
2.4	Information-as-a-Service	Five	[29–33]
2.5	Process-as-a-Service	Five	[10, 34–37]
2.6	Application-as-a-Service	Three	[38–40]
2.7	Platform-as-a-Service	Four	[41–44]
2.8	Integration-as-a-Service	Four	[45–48]
2.9	Security-as-a-Service	Ten	[49–58]
2.10	Management-as-a-Service	Eight	[2, 8, 59–64]
2.11	Testing-as-a-Service	Three	[10, 65, 66]
2.12	Infrastructure-as-a-Service	Four	[67–70]

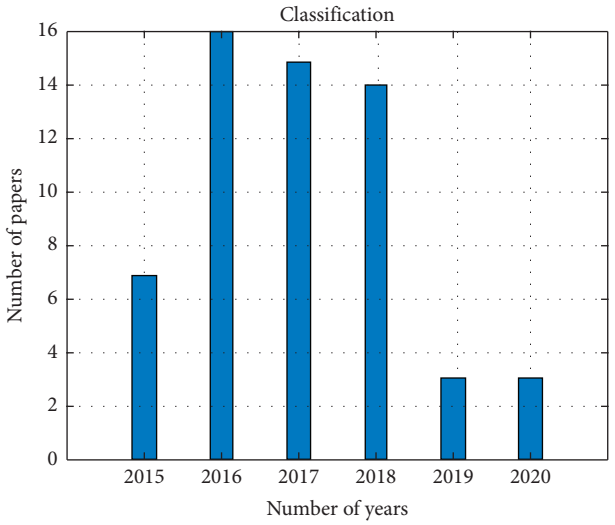

Figure 3: Classification of the related work.

gigabytes. The AES algorithm is used to encrypt the data. This work efficiently secures the big data. However, small data encryption is not discussed.

In [24], the data classification-based secure cloud computing model is proposed. The previous approaches regarding storage frameworks use the same key size for the data encryption without looking to the confidentiality level with an unnecessary overhead as an output which increases the processing time. In the proposed framework two important issues of mobile cloud computing have been solved: one is called security and the other one is called storage. For the confidentiality of the data, an efficient framework is proposed which provides strong confidentiality to data and integrity in the cloud storage system in both aspects, i.e., transmission and storing operations. Along with it, this framework reduces the processing time to encrypt the data and complexity. Internally or externally of a cloud system, all the threats are hacked in an efficient framework. The second is without taking the confidentiality degree when the encryption of the data is performed. To tackle this problem the proposed framework includes the algorithm which enables the user to encrypt its data with a key that is not available to any other person. Huge data, i.e., 100 gigabytes in a combined form is difficult to encrypt with the same key; therefore, a cloud storage model is proposed which includes three levels to encrypt the data with confidentiality. The three levels are basic, confidential, and high confidentiality. The idea of specifying in the confidentiality level of data follows in the proposed work which is called the manual classification. For the encryption of data, different cryptographic approaches are used called AES, TLS, and security hashing algorithm (SHA). The data with higher and lower critical values will be stored on faster and slower media, respectively. In short, an efficient confidentiality-based cloud storage framework is proposed, which enhances the data encryption process time and integrity. The high data confidentiality and integrity is achieved.

The cloud is mostly used to store and process big data. In [25], the authors propose a big data division mechanism. In this model, the big data is divided into small sequence parts

and then the sequenced parts are stored into different multiple CSPs. After the division of big data, the divided big data sequences are collectively combined with their sequence and stored on different cloud services. There are two types of storing the data on a cloud service: one is public data and the other is confidential data. The public data is accessible by any user and it is open to all, while the confidential data can be accessed by the relevant users. To make the big data of tenants secure, a secure cloud big data cryptographic-based virtual mapping storage scheme is proposed. In this scheme, the big dataset is divided into sequential data parts with a certain principle called the same data-type block or IP resembled. The big data of tenants divided into n sequenced numbers, where each divided sequence of big data stored on m different storage providers. A unique storage path for big data is formed when the big data is stored. The trapdoor functions are used to protect the mapping of various data. The trapdoor functions are widely used in cryptography. It is difficult and even impossible to secure or encrypt the big data as a whole, so we only need to encrypt the storage path of the big data, and according to this, we can obtain a cryptographic value called cryptographic virtual mapping of the big data. To more improve the robustness of the proposed work, the model stores multiple copies of each data on different indexes of the providers. If one data is lost or missed, then the cloud checks the missing data sequenced number in different indexes and tries to recover and store it on the relevant provider. The simulation results show that the theoretical proof analyzes the model in an efficient and secure way. Two different scenarios are considered, and comparing these two scenarios with the related approaches finally proves that the proposed scheme is more effective and feasible to protect big data for cloud tenants.

In [26], different security services are discussed using a sequence of game models amongst the cloud user and provider. The security assessment model is used with the help of which users can find the risks of their data privacy which is likely to be hacked by cloud. By taking into account the security of the data amongst cloud user and provider, this work investigates three types of scenarios, which are one user, multiuser model, and multiservice provider. Different series of models has been discussed to develop the security for CSPs and TSPs. In the first game model, a game is established between one user and a cloud provider. The user has the choice of whether to use the cloud services or not while on the hand the cloud provider has the choice to steal the data of the user or remaining host. In the second game model, there are many users and only one service provider. If the data of one user has been stolen by the service provider, then all the other users lose the trust of the cloud provider. In the third game model, many users and many cloud providers are discussed. The utility function is used to differentiate the incentive for each user and provider. In this, the relation of all users and providers is not the same and is classified into competitive, cooperation, and dependent. In the first one, different providers provide their services, terms, and conditions. In the second, the users can use the sources of all providers. In the last classification, the providers serve as the third party.

2.3. Database-as-a-Service. Table 5 presents the short summary of the Database-as-a-Service classification.

In [5], the pricing and investment problems between the cloud insurers and the users in a cloud market are proposed. The cyber threats are responsible to damage the cloud user's data. The market includes users, cloud providers, and cloud insurers. The cloud providers provide cloud services to users. The cloud insurance has a product which the users buy to protect their data from damage. When an attack happens to the cloud service, then the cloud insurer pays a claim. The users are dependent on each other in which they can take the benefit of the security effects which are produced by the other user's investments in security. In this model, it is assumed that the cloud provider and the cloud insurer are the business partners. Therefore, to improve the security levels, the cloud insurer charges the cloud platform, i.e., to enhance the quality of the cloud service and reduce the paying claim probability. The Stackelberg game is proposed in this model which has two stages. In the first stage, the price charging is set on the users by the cloud insurers and the improvement in the cloud security quality decides by the investment. In the second stage, the users decide on cloud insurances to purchase based on the observed prices and qualities. By applying the game-theoretic approach called the backward induction, the optimal pricing, security investment strategies, and optimal strategies of the users are presented. The NA of the game regarding the best responses of the users is found. The best response of each user can be found by taking the derivative of the utility function concerning for to function on demand. The simulation result shows that the Stackelberg model is proposed to maximize the utility of the users which correspondingly maximizes the profit of the cloud insurers.

In [27], the authors propose a pay-per-use IM-SecaaS model for cloud security. The architecture of the IM-SecaaS involves the main components: intrusion detection, intrusion response, reporting, and logging. Before the data reaches the users, the model checks and cleans the data by monitoring web traffic or the attackers attack the data. There should be no investment for anything on premise solutions. However, the client should pay based on the pay-per-use model. IM-SecaaS is provided as a service for the users, so, in this case, the users should pay in the form of OPEX. The model is proposed for Pb in which proof of concept prototype is implemented. The function of the IM-SecaaS is like the policy administrator. On one side the public Internet is input to IM-SecaaS where doubtful traffic comes while on the other side the client organizers are present. By applying all the policies on the input doubtful traffic, it becomes clean and then delivers it to the client. On a virtual machine, the model is implemented in a Pr. Both the IM-SecaaS core and IM-SecaaS managers have been implemented in different virtual machines. The IDPs from multiple vendors are more efficient than using it for a single vendor. The uninterrupted service is provided to the cloud by proof of concept (POC). The model enhances the flexibility, control, privacy, and cost for a Pr.

In [28], the authors trying to solve some security issues regarding errors of screening indicators lack validation

Table 4: Storage-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[20]	The model presents different security policies on the cloud storage and data; the data is not secure everywhere in the cloud data which is fragmented for security purposes; the identity authentication is used for security	The model analyses the cloud storage different methods are applied at different stages to achieve security	The data transmission encryption, access control, identity authentication, and Shamir's threshold secret sharing program are used in the presented model	2017
[21]	The data placement problem is addressed for the big data in the cloud storage system; the data placement problems are solved by the decision, size, and number of chunks	The renewal time minimizes up to 20 percent and 21 percent for the network and Internet topology, the linear programming model, heuristic algorithm, and T-coloring approach	The linear programming model, heuristic algorithm, and T-coloring approach	2016
[22]	As the cloud network is an open platform for the users to store and compute the data; the users store and compute the data in the cloud over a wireless remote network by using the Internet; security of the data is the concern in an open system for this purpose encryption and decryption of data outperformed to secure the data	Different steps involved in the proposed work which strongly secures the data from the start to end of the system	Encryption and decryption of data with integrity are applied	2017
[23]	Several different security issues are discussed in this article; after that it proposes its own work; the data is divided into small and large sizes; the symmetry encryption approach is applied to large size data	A strong encryption on data applied which fully secures the larger size data from threats	The AES symmetric encryption algorithm is applied to the system	2015
[24]	The proposed work targets the two main security issues called the confidentiality level of data and data encryption processing time; the key provided to the users which are not for to avail by any other user	The data encryption time and overhead reduced by achieving a reliable cloud network	The AES, TLS, and the secure hashing algorithm (SHA)	2016
[25]	The big data is divided into n sequences and stored in m different CSPs which is proposed to ensure the security of big data; the cryptographic virtual mapping and trapdoor techniques are proposed to achieve high feasible protection of the big data	Two different scenarios are analyzed in the proposed model, and the simulation results concluded that the proposed model provides more security for big data in an efficient way than the other traditional approaches	The cryptographic virtual mapping, data type block or IP resembles, and trapdoor function	2016
[26]	Three game models are discussed to analyze the security in the cloud system; the assessment model helps the users to find the risk of data privacy	This model ensures the privacy of the data and hence minimizes the influence of the third party in private data	Security assessment model, one user, multiuser, and multiprovider	2019

reputation scientifically. Based on these issues, a well-reputed security model is presented using S-Alex Net convolution neural network and dynamic game theory called SCNN-DGT. These algorithms are used to privatize the health data in the Internet of Things. The proposed model is classified in two different stages; firstly, the health data information of the user is arranged using S-Alex Net; secondly, game-theoretical approach is used. In other words, for the sake of data security from harmful identity game, a theoretical approach called security reputation model is used and hence data security is improved. For learning invalidation which is caused due to small matrix features, S-Alex Net neural convolution is used. Moreover, this paper presents the SCNN-DGT model which includes three stages: predispose stage, big data security stage, and early warning supervision.

2.4. Information-as-a-Service. As a summary of this classification component, Table 6 is shown.

In [29], the authors propose a new attribute-based sharing scheme used to resolve the security issue while the data sharing is performed in a cloud. The data sharing on a cloud becomes more popular due to its low cost. To share the data in a fine manner attribute-based encryption (ABE) gain more attention. The previous ABE

Table 5: Database-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[5]	The SSG is proposed for cloud security; the defender and attackers are compared by applying the model; the utility function, best strategy, and payoff are analyzed in the game model	The information on the attacker's behavior is collected by active and passive stages of the SSG; the efficient utility function is achieved by this model; the defender availability and cost are maximum and minimum, respectively	The security Stackelberg model, active and passive stages, utility function modeling, natural roles, and defense strategy	2018
[27]	This model works on a pay-per-use basis; doubtful traffic enters at one side of the model by applying different policies by the model components; a clean output data is provided to the clients	The model not only improves the security but also the flexibility, control, effectiveness, and performance as well	The IDPS and POC are used in this model	2016
[28]	This proposed work aims to manage and secure cloud data; incorrect screening and privacy of the cloud data is encountered	The outcomes of the experiments show that the proposed model solves the problem of low accuracy and reliability of the data in the cloud environment	The neural network model called S-Alex Net and game-theoretical approach SCNN-DGT is discussed	2019

presented by the researchers has the disadvantages of high consumption overhead and weak data security. The proposed work addresses these challenges by introducing a new ABE technique with additional features. By the addition of the system public parameters, the computation task has been eliminated with partial encryption consumption offline. Most of the computation overheads are eliminated by adding the public ciphertext before the decryption phase. Furthermore, for more securing the data, a chameleon hash function used to generate immediate ciphertext which is blinded by the offline to obtain online ciphertext. For the ABDS for mobile users, the new online/offline ABE scheme introduces to eliminate the moving encryption computation overhead on data at the owner side to the offline phase. The public ciphertext enables the user to check the cost of whether the equation holds a low cost or not before going to expensive decryption. The proposed framework is proven that the chosen ciphertext attacks (CCA2) are recognized as a standard security notion. Both experimental and theoretical results prove that the ABDS system outperformed resource-limited mobile users in cloud computing. The simulation results show the proposed work stands well regarding cost in the online and offline encryption time.

The data security is linked not only with the CSP but also with the user concerning data at rest, transferring data, and processing the data. In [30], the BPMN for the cloud data security is presented. The aim is to provide security to the cloud data; for this purpose, two types of CSP are used called CSP-1 and CSP-3, while the CSP-2 is disclosed and does not provide information for academic publishing. The BPMN can point out the section which is affected by the security attack and hence save the time and resources of the attack to perform recovery actions. In BPMN, large-scale penetration testing performed to test the power of the security system and service. The BPMN model is used effectively for the security business organization. For this purpose, the BPM is used for the security of the cloud. Bonita soft is software used for business process management (BPM) modeling and SSDP. The BPMN is used to simulate the data security for the three CSPs called CSP-1, CSP-2, and CSP-3. These service providers get the security data designs partially from the service providers and partially from the users. The CSP-1 is responsible for secure delivery and high-level services such as networking, storage, database services, infrastructure, and computing to the cloud system. It focuses on the data security model shared between the provider and the client. The several stages of data security and transfer security are performed by CSP-3. It incorporates the security policies, company structural security, data management, access control, personal, physical, environmental, and infrastructure securities. In short, the business security model proposes using CSP-1 and CSP-2 models. In the first case, the user requests the service provider after which it enters into the system and passes through different several management and security checks. In the second case, there is no request to enter into the system, but the request for logging into the client system. After the completion of these two cases, the whole data passes through many layers for the security purpose; if any layer misses the data, then it passes through the ADIRS. This type of model is applied in the health sector, national security services, banking, and many other companies which store confidential data.

The proposed framework achieved a minimum makespan and maximizes the reliability by assigning different tasks and data blocks in a cloud system [31]. The proposed framework tries to tackle the NP-hard problem; for this purpose, different intelligent computational algorithm such as GA, PSO, and ACO are proposed. The ACO is a probabilistic algorithm used to find the optimal path in a graph by the behavior of an ant colony. The ACO has many properties with the drawback of stagnation in the evaluation process. To overcome this problem, chaos factor is introduced. The CAS is a heuristic random search algorithm based on intelligence theory which affects the evolution of an ant colony

Table 6: Information-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[29]	To tackle the problems of computation efficiency and weak data security, ABDS scheme is proposed in cloud computing; the users are enabled in this approach to check the cost of the ciphertext in online/offline encryption mode before going to expensive full decryption	The users can get online and offline encryption with minimum cost and time; the proposed work gives strong security to weak data	The ABE, attribute-based data sharing (ABDS), chameleon hash function, and online/offline ciphertexts	2018
[30]	The framework used two types of CSPs to secure the cloud data while sharing the data and passes through several stages; the main focus is to provide security to the big data system	The model highly provides security to cloud data services such as storage, networking, data management, access control, and infrastructure security	Bonitasoft, business process management, CSP-1, and CSP-2	2016
[31]	To tackle the NP-hard problem, a series of MHAs, characteristics with a simple structure, fast confluent, and energy have been proposed; the MOO problem solved in terms of reliability, make span, and time	The proposed CAS solved the problems of the salesman, economic dispatch, and fuzzy system identification; the ACO finds the optimal path in a graph investigating the behavior of an ant colony, make span and flow time analyze the reliability factor	The ACO, chaos factor, make span, time flow, and GA-CAS	2016
[32]	The proposed work highly secures the cloud data; in this work, the data is split and then distributed by different cloud servers; the paper tries to resolve the abuse issue; the direct access of the cloud to the user's original data is prevented	The experiment proves the proposed work efficiently performs this task by consuming less time as compared to AES	The algorithms SED2 and EDcon	2016
[33]	The US government data is protected from advanced persistent threats (APTs); the cloud security assessment model is used for four multitenant IaaS cloud architecture	The CCS penetration probability is high if minimum security control sets are applied	The cloud security assessment model, APTs, and virtual machine	2017

from chaotic to individual self-organizing in a random search process. The CAS evolution involves two phases called the chaotic phase and the organization phase. Besides this, the Markov-based method is proposed for reliability. Furthermore, in the GA-CAS algorithm, four operators and natural selection are applied to solve the MOO problems. The four operators according to the characteristic of the cloud scheduling problem enable the CAS to solve the combinational optimization problems. The task scheduling problem in cloud computing is solved by the proposed MOO model. The user's task is taken into account in a multi-objective model and illustrated the scheduling performance in terms of make span, flow time, and reliability by applying queuing theory and Markov process. The make span and flow time encounter the reliability factor as follows: (a) only one task can be executed by each node at any time, (b) the links or communication links are independent of each other, (c) there is no discontinuity in the process of subtask execution, and (d) all nodes play their own role, and there is no useless node. even a series of tasks are inputted to the model. The simulation results concluded that when the proposed GA-CAS algorithm is compared with the other meta-heuristic approaches, it outperforms in solving the task scheduling problem of a cloud system.

A novel-based approach is presented in [32] to provide high security and an efficient mass distributed storage (MDS) service to the cloud data. The anxiety and adaptability of the users can be increased by cloud if the cloud operator directly reached to sensitive data. The paper mainly focuses on this issue; therefore, a novel approach is proposed to overcome this issue. The proposed algorithm efficiently splits the files and data which store separately on the distributed cloud service. In this phase, data is unable to reach the cloud service operators directly. Two main algorithms worked in this propose article called SED2 and EDcon. The framework targets the problem of abuse issue. All the data, encrypted and distributive, is stored on the different cloud servers without causing any big overhead and latency. The SED2 algorithm splits the data to prevent the data from leakage by using minimum cost. In executing the SED2 algorithm, two other supportive algorithms are used to encrypt and decrypt the data in a good way. In summary, the whole framework was proposed for the two main points. In the first, the proposed work prevents the cloud provider to reach directly to the original user data. In the second, a highly efficient mechanism is used to split the data which never produces big overheads but ensures data retrievability. The experimental results show the proposed work is compared with AES. The execution time for the proposed work is much lesser than the AES algorithm.

The vulnerabilities to advanced persistent threats (APTs) in cloud computing systems (CCSs) are important.

The reference model of the cloud covers and controls the security. In [33], the cloud trust assessment model is proposed to estimate the high-level security which is a high quality of confidentially and integrity by a CSP. The proposed model can access the security levels of four multitenant IaaS clouds which have alternatively equipped architecture for the cloud security model. The proposed CCS reference model and an assessment model ensure high security to IaaS, CCSs, and CSPs. Cloud tenants can be used to decide on which one CSP security features need to implement. The proposed CSS four architectures are designed to protect the government official data, and then they are practically implemented in the US. Whether these architectures successfully protect the US government official data has been analyzed. It is based on the BNM of the CCS. The spanning of the CCS attack is carried out by the APT. Each attack path needs the space, and the APT attack steps to implement. The CCS secrecy status is summarized by the two key security metrics: the first one is the chance when an APT can access high magnitude information. The second is the detecting chance of APT by the cloud tenant. In first security metric checks, high magnitude data called "Gold" information weather adjusts or is deleted from the CCS. The second metric assesses the analysis of cloud monitoring tenants, file approach, and alertness data to find intrusions into a tenant's cloud network, whether they contribute to intrusion detection or not. The results show the penetration probability of CCS is high if a minimal set of security controls are implemented. The CCS penetration probability drops substantially when the cloud protection in depth security is adopted which protects the virtual machine images.

2.5. Process-as-a-Service. In Table 7, the summary of this classification is shown. This summary is based on the references, overviews, techniques, advantages, and papers' publication year of each paper cited here. Cloud service becomes more popular due to highly upgrade of information technology and due to low cost, service on demand, high service scalability, and many more. However, security and privacy are not completely provided yet. In [34], the new security and privacy model for cloud service are provided. The proposed model is called CSPM. The NIST provides the main structures and buildings for the cloud called services, deployment models, and characteristics. The services for the cloud are security as a platform, infrastructure, and software. The deployment models include public, hybrid, community, and private. The characteristics are five in numbers and called on-demand self-sourced, broad network access, resource pooling, rapid elasticity, and measured service. The proposed models investigate different threats and give valid solutions for the corresponding threats. The security issues are ACPML, data (geographic, integrity, loss, privacy, and physical), environmental security, and proactive threat. The CSPM consists of five layers called physical and environmental security, CI, network securities, data and access control, and ACPML. These layers introduce the security policies, management, and monitoring steps for the cloud service. These layers are investigated at every stage of the cloud by the proposed model and make the difference between the attacks threaten availability and security along with the countermeasures which provide the security services to their clients. The model helps the CSPs in terms of security management and privacy. And the monitoring of cloud facilitation can be achieved. The threats and attacks in a cloud system can be insider attacks, cloud malware injection attacks, and cryptographic attacks. In short, the layered model presents the threats and attacks along with the countermeasures.

The novel scheme called attribute-based encryption (ABE) with the policy updating method is proposed in [35]. It mainly focuses on access control in an efficient manner with the updated dynamic policy for big data. In the proposed approach, the computational work minimizes due to avoiding the transmission of encrypted data and by using previously encrypted data with access policies. For different types of access policies, different updating algorithms are proposed in this work. The grand challenges in policy updating are correctness, completeness, and security. The correctness is the ability of the users who possess the attributes and are able to decrypt the encrypted data under the new access policy. The completeness is the method of policy updating which have the ability to update any type of access policy. The security of the access control system should not break by policy updating. The main goal of the proposed scheme is to solve the problems in policy updating using ABE systems. Firstly, the formulation has been done of the policy updating problem in ABE systems, according to which new methods are developed to outsource the policy update to the server. An expressive and efficient DAC scheme for the big data is presented through which dynamic efficient policy updating can be achieved. For different types of access policies, different policy updating algorithms are proposed such as Boolean formulas and access trees. The proposed algorithm not only satisfies all the above problems but also avoids the transferring of encrypted data in back and forth shape. The policy updating problem in big data is incorporated in this proposed scheme. Furthermore, a method is proposed which enables the data owners to check the correctness of the ciphertext updating. It also provides the safety in terms of the data owners, i.e., it cannot use their SKs to decrypt any ciphertext encrypted by other owners, although their SKs contain the components with the attributes. Although, in the designed policy, updating algorithms is based on water. In short, the simulation results prove that the proposed scheme is good in terms of cost, ciphertexts updating, and policy checking. Also, the proposed scheme provides the correctness, completeness, and security to the big data.

The demand for cloud service increases day by day according to the demand for cloud services; they provide enhance scaling, agility, availability, and flexibility. However, the cloud has some issues which are to be improved: load balancing, security, and fault tolerance. In [36], Rahul Rathore et al. presented a cluster on geographical-based dynamic distributed load balancing technique. The job assigned to each cloud provider is 100 in length and the distributed arrangement is chosen for all cloud servers. If the job number 101 has arrived at any service provider, then cluster applies its load balancing algorithm. In this model, a security mechanism is also introduced which secures the

Table 7: Process-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[34]	The model investigates different security and privacy issues; in this work, five layers are introduced which protect the cloud system at every layer from threats and attacks	This model provides a secure service with confidence; it provides the difference between attacks and security along with the countermeasure secure services	The model used five different layers to protect the cloud from threats called the CI, CISL, PESL, data layer (DL), and ACPML	2016
[35]	The policy updating problem in the big data is solved by proposing the attribute-based encryption (ABE) scheme; then, DAC scheme for the big data is proposed which enables the owners to dynamic policy updating; different policy updating algorithms for different types of access control are proposed	This approach enables the checking of directly updating ciphertext by the cloud; there is no need for policy updating in data decryption	The outsource ABE, DAC scheme, Boolean formulas, and access tree	2016
[36]	The static and dynamic load balancing techniques are proposed; the pairs of keys are generated to secure the data; load balancing attached to a cloud effectively avails the resources provided to nodes	The model performs better in terms of response time, throughput, resource utilization, fault tolerance, and scalability	Load balancing technique, dynamic load balancing, and key pairs	2018
[37]	The data security monitoring method based on autonomic computing is proposed; different modules are proposed to gather the data stream and then evaluate the processed data to determine the abnormality; the data collection and analysis of storage are the core of the proposed model	It can accurately evaluate the degree of abnormal; the cost can be reduced by the architecture of integrating modules	The data monitoring process on autonomic computing and data mining algorithm based on the chaotic algorithm and abnormal behavior detection based on Poisson	2018
[10]	The sharing of data between a mobile system and cloud system is discussed in this work; the AES technique is used to encrypt the high definition (HD) video; different keys are used to make secure the system are public, private, and security keys (PUK, PRK, and SK)	The delay minimizes due to utilizing the computational power	AES, HD video, HEVC, PUK, PRK, and SK	2017

data transmission between the user and the service provider. A key generation process to encrypt and decrypt the data has been applied which is valid to perform this job. A pair of keys with a password or PIN is generated to completely perform the job of encryption and decryption of the data between each the user and the cloud. The load balancing is a technique used to balance all the load of the server on the nodes and gives all resources to nodes, which minimize the time response. The solution of overload, under load or dill server, is presented in the proposed model. Dynamic load balancing has four main steps. In the first, the transfer strategy is discussed to transfer a job from local to the remote node. In the second, the selection strategy is discussed to choose a perfect processor that performs well according to the input job. In the third, the selection of destination is introduced. In the fourth, all the information of nodes is collected in this stage. The cloud is arranged in a cluster form and the cluster is arranged in a hybrid form, i.e., hierarchical and distributed manner. The service array of each cloud provider is zero initially. When a user wants to avail the services of a cloud, then it requests to the cloud. Then, the service array checks by the cluster head if it meets the user array or not. If yes, then it can avail the service, otherwise it avails the services of service provider. This checking of service array repeated until the CSP is selected for the user. The authentication server has the password of the users which are particular to service providers. The client enters the authentication password which perfectly matched; hence, the cloud service is open for it and the data is made secured by the user. The proposed framework outperformed in throughput, overhead, fault tolerance, resource utilization, response time, and scalability.

The data stored in the cloud platform may be affected by the attacks; therefore, data monitoring is a necessary process. In [37], a cloud data monitoring system is proposed on the cloud platform. It monitors the cloud data whether it is abnormal or not and then analyzes the security of data according to the monitoring results. The proposed approach mainly focuses on the security of the cloud data; for this purpose, the approach follows different steps. The approach

proposes a model which efficiently and safely monitors the cloud data on time. The system adjusts the monitoring system in such a way that it automatically protects the data. The approach proposed a mining algorithm in which an improved-based chaotic algorithm, data mining method is proposed for the appearing of abnormal data in the cloud. To obtain the accurate test results, the approach also designs abnormal behavior detection based on the Poisson. All abnormal behavior monitoring data security implemented on autonomic computing. The model is mainly composed of five different modules called the NMM, the data analysis module, the response strategy module, the system implementation module, and the knowledge-based module. The NMM is used to gather the data of the system by collecting the data stream and generates the original data. The processed data is evaluated and extracts useful information by the data analysis module to determine whether the data extracted is abnormal; then, this data is fed back to the response strategy module to adjust the monitoring period. The core of the proposed approach is the data collection and analysis of storage. These two provide essential data monitoring information. In short, the idea of abnormal data monitoring and autonomic computing system is proposed. Then, the data security monitoring method based on autonomic computing is proposed. By doing this the changes of data in the cloud are monitored to ensure security. The simulation results show that the cost can be controlled and reduce with the architecture of integrated modules of collecting data, analysis, monitoring service, and volume-based monitoring cycle adjustment.

In [10], the sharing of data between the mobile and cloud in the secure lightweight, robust, and efficient schemes is presented. The media files such as video, audio, and images can be uploaded to or from wireless servers. The transferring of data between mobile and cloud should be authentic and free from risk. Previously, all presented schemes regarding the sharing of data between the cloud and mobile have the limitation of memory support, processing load, and data size. This framework considers the HEVC with IEVS for data hiding. The AES technique is used to encrypt the data in the proposed framework. The analyses of the work are to implement this model in real-time processing in such a way that the energy cannot be consumed more. A lot of abundant information is contained by high definition (HD) videos; the intradomain is used to encrypt the video as a result of which more compression occurs, and it also provides an extra slot for abundant to hide the secret data. The cryptographic approach is used to encode the HD videos; it creates the overload on the input video sequence in execution on the mobile devices. The encrypted data are then shared on Pb which is semitrusted for downloading the uploaded videos; the public key (PUK) and the private key (PRK) are provided, which will decrypt the video instead of encoding. The decryption is performed only by an authentic user who has SK. An extra feature has been introduced in the proposed framework in which the user mobility can be traced by authenticating it remotely. The PUK, PRK, and SK do not acquire any synchronization at any stage. An uploading user is responsible to encrypt and upload a video and must be announced to all the other authentic users that a new video has been uploaded. It is a choice of the user whether he wants to download and decrypt the video or not; the video can be decrypted by the SK. The proposed work performs his job in an efficient way in the Pr, i.e., the model saves the computational power in a cloud system while the decryption of the data performs. It is not necessary for the presented model that the receiver must have the same computational resources as the model has for the encryption process. The simulation results show that the processing time decreases up to 4.76 percent, correspondingly the data size approximately increases up to 0.72 percent, and the proposed framework applies to real-time cloud media.

2.6. Application-as-a-Service. Table 8 shortly summarizes the application-as-a-service. The abstraction layer system and method used to secure cloud computing is presented in [38]. The development and deployment of at least one software workload for a virtualization environment are presented. Through the software policy, for a workload associated with a metamodel virtualization environment, a security zone is defined by the developer. And then apply at least one type of security policy with respect to the security zone including all types of security zone policy in the metamodel. In such a way, the security zone policy can be associated with the development of the software workload. If the security zone is related to the software workload, then it automatically applies the security policy when the software workload is deployed within the security zone. The preference for an infrastructure environment is decided by the software development life cycle. This includes the definition of security, policy, and management. Unlike previously presented algorithms, in the proposed work, a user can plan a cloud, build a cloud, publish a cloud, service by consumption, or run the cloud computing service. The best fit values can be selected between the internal and external service providers. Several modules are used to perform different actions on a cloud system to ensure security. Consumption module 32 is used in collaboration and to access the cloud service published for consumption. Module 26 called a manager module is used to configure one or more clouds for services or computer workload to monitor the cloud.

The connected vehicular cloud computing (CVCC) a hybrid technology used for the security and privacy of the cloud model involves computing resources such as the cloud, roadside infrastructure, and vehicles presented in [39]. Unlike the traditional cloud, the proposed CVCC vehicular resources include applications and possible services when the cloud and roadside infrastructure are not available. On the security and privacy challenges of the CVCC, researchers pay attention to the advanced cryptographic primitive technique. In this technique, pairing computation consumes more time; therefore, it is good to use outsource pairing computation for the vehicles. The primitive is built on bilinear groups called G_1, G_2, and G_T. The first and last groups are additive cyclic and multiplicative cyclic, respectively. In CVCC, the time

Table 8: Application-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[38]	The visualization environment is used to update the development and deployment of a software workload; different zone security policies are adopted by the metamodel framework; the SDLC used to find perfect infrastructure environments	Highly improves the security of cloud computing	The SDLC and different cloud modules are used, i.e., builder module, consumption module, and manager module	2018
[39]	Three different entities involving cloud, roadside infrastructure, and vehicles with additional work of advanced primitive cryptographic primitive make the connected vehicular cloud computing more secure and confidential	The service of the CVCC provides more reliability to the cloud users due to the availability of the service even in the absence of cloud and roadside infrastructure	Advanced cryptographic primitives, outsource pairing computation, and rich applications	2018
[40]	Different algorithms and steps are proposed in cloud security; among them, one algorithm is proposed here; the security uses service level agreements; in this work, two techniques called the QPT and QHP are used on the cloud system	This proposed work ensures the security of the user's data at different levels	The SecSLA, QPT, and QHP are applied	2017

consuming in the bilinear groups is the pairing computation for the vehicles. Three different kinds of entities in CVCC are used called the cloud, the roadside infrastructure, and the vehicle. Among these three entities, the cloud has the most powerful computation capability. At second, roadside units (RSUs) have the powerful computation capability. And these two entities act as a server in pairing outsource services. The cloud is used as a helping model for the rest two entities such as the vehicles update their system through the cloud. The roadside infrastructure has many RSUs, and the roadside infrastructure provides all the services to the vehicles. The proposed framework has two kinds of pairing outsourcing models. Among these two, one is is outsourcing the pairing computation with only one server and the other is with two servers. In CVCC, every server vehicle acts like a malicious. Hence, the second outsourcing model not completely fits CVCC. Compared to the traditional cloud, computing the CVCC is superior in developing secure cloud data center model and Big Data concept analysis. According to the input properties, the pairing computations have seven types, but the proposed framework is related to only one amongst the seven.

The economic and technological benefits are not attractive in front of the security issues of the CSP. However, different steps or algorithms and software are developed to minimize security issues. One of them is SecSLA. In [40], the two-state of art security evaluation techniques are called the QPT and QHP. The QPT and QHP techniques are applied to cloud systems to provide quantitative- and analytical-based security. These techniques provide flexible security to ensure users using CSP. The extension is carried out in the proposed framework regarding the state of the art and standardization. The QPT and QHP techniques are empirically validated through a couple of case studies using real-world CSP data obtained from the CSA. The limitation and advantages of the QPT and QHP can be analyzed by experimental validation of these algorithms to further guide the adopters. The visual security can be judged by the users in CSP through the prototype of decision-making security. Overall, the system security is in the satisfaction category judge by the users. The techniques provide security insurance at different levels. However, the security evaluation is not in an end-to-end domain.

2.7. Platform-as-a-Service. Table 9 is provided for the ease of this classification component, which summarizes this component in a short way. The two heterogeneous tasks are presented in [41]. These algorithms are cost paying and the users should notice the cost while renting the virtual machines from the cloud data centers. The workflow is heterogeneous and needs different instantaneous series of computing, memory, and storage optimization. The proposed work is based on different optimization techniques called metaheuristic optimization technique, PSO, and the coding strategy. Through the PSO, various tasks are mapped corresponding to the virtual machine in terms of pricing. These optimized techniques minimize the cost of the total work-flow execution while providing the desired deadline and risk rate. The cloud features include dynamic provisioning and the unlimited heterogeneity of computing resources along with the hourly pricing model. To meet the desired requirements, the scheduling and resource provisioning methods are used into MDMCO problems. The coding strategy for PSO workflow scheduling has been applied to solve MDMCO problems. The practicality of the proposed model is using the three different real-worlds and workflow applications (LIGO, SIPHT, and Cyber-Shake)

Table 9: Platform-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[41]	The risk rate and cost are analyzed using three different workflow techniques using cloudSim simulator; the workflow needs a periodically based series of computing, storage, and memory optimization	This framework provides risk minimizing according to the cost for a user in the cloud	The MHA, the PSO, and the coding strategy	2016
[42]	The authors propose a new framework to provide managed security services via SDK; different techniques are involved in outperforming the model; the BT works to provide security to data for Pb and Pr in a multicloud environment	Through this model, a user can secure its data for different cloud services such as private, public, and hybrid	The horizontal service model, BT service store, and managed security service obtained through SDK	2016
[43]	For the data security purpose, encryption technique is applied in this presented work; the encryption approach is applied using AES	The algorithm provides strong security for data in SaaP	AES algorithm is applied to the cloud system	2018
[44]	Three best strategies are applied to achieve the best response in data security and openness services; then, between these two, a relation has been drawn to help the cloud provider to choose the best strategy for both security and service	This proposed work decreases the investment for the security purpose and puts the cloud user in optimal service openness and best security environment	Specific probability with macroanalysis, best strategies for investment in terms of security, and Nash equilibrium	2019

on the cloudSim simulation to demonstrate the effectiveness of the risk rate and cost.

Not only the security of the cloud is important but also financial discipline has the main role in SaaS and PaaS. In [42], the horizontal service model is designed to investigate how the managed capabilities migrated as security applications via software development kit (SDK). Through this approach and its associated SDK, the customers are allowed to implement and enforce different security policies to a Pr, Pb, and HCs. The reassurance of business continuity by protecting the application level of Iaas and Paas has been achieved by the cloud computing security model. This model provides the high security model with the structured methodology that the customers will like our cloud applications. The model provides CEPM along with the information technology (IT) cost optimization to the security budgets. The BT service store is a web portal that contains applications and where the customers can configure a Pr and Pb. BT is responsible to make security at the customer's end. BT has a set of security solutions via the horizontal model. In the proposed model, the security enforcement issues and compliance are demonstrated and show the elasticity, load balancing, and indeed security. The integration of the service store will be carried out through SDK. However, much software are assumed to be present in SDK because HS is accessible remotely, and there is a separation between management and enforcement configuration. The SDK involves the capabilities of deployment, enforcement, disablement, and removal. The proposed framework is flexible and can support any kind of security solution regarding any cloud platform through SDK.

In [43], the Heroku cloud is considered the service as a platform (SaaP). The dyno app is responsible to run the Heroku and this app is like the heart of Heroku. It supports different types of programming languages. The strongest is the cryptographic approach called the AES which is applied. The AES is a concern with the security, speed, and symmetric key algorithm. The Heroku contains different steps that make the data secure in SaaP. One step is the replacing of each byte with the byte of the substitution table. The second step is the cyclically shifting of row towards the left. The third step is a fixed polynomial which is multiplied by each column.

A complete security control and complete service openness are presented using Nash equilibrium in terms of investment in service, and security by cloud system is presented in [44]. Two assessment methods based on quantitative analysis have been accomplished for the investments. Amongst them, one is for security and the other one is for service openness, which are discussed. Then, a relationship has been drawn which helps out the cloud provider to make a decision: the best strategy in terms of both service and security. However, openness brings security problems in terms of illegal benefit. To make sure the security investment increases which helps in improving the security detection technology, there should be a balance between these two, i.e., investment and security. Therefore, this proposed model decreases investment and security investments. Three optimal strategies are applied to meet the desired response in terms of best service openness and strong security which are provided to cloud users. Firstly, the macroanalysis has been carried out with specific probability. Secondly, the best investment strategy is accomplished to

meet balance investment for security and services. Thirdly, the Nash equilibrium point is calculated to fulfill the optimal service openness and security conditions.

2.8. Integration-as-a-Service. In order to shortly analyze this classified component, Table 10 is provided. The CCAF security suitable for business clouds is present in [45]. Three major security technologies are developed and integrated with CCAF called firewall, IM, and encryption based. All technical issues in a cloud system are analyzed here, and the model is a business-based cloud. The framework provides its explanation with the help of three examples. In the first, the framework gives a solution for bioinformatics and cloud storage. All structured query languages (SQL) are blocked, which protects data in real time in CCAF multilayered. The bioinformatics service can simulate DNA, proteins, genes, tumors, and many other organs of the humans. In the second, CCAF is also used as a guideline for financial modeling; the price and practice are changed according to the risk. In the third, the model investigates the hacking methods as a part of prototype requirements. In CCAF 1.1 version, different techniques are proposed, namely, security policies and recommendation techniques, and the technologies are updated and emphasized. In this framework, mostly advanced computational techniques are discussed and used for the calculation of the risks and the volatility of the market. The proposed concepts are essential for big data in a cloud system. The backup of thousands of terabyte in size is delivered to storage services. The framework provides security assurance to all incoming and outgoing data to cloud systems which are based on thousands of virtual machines. By using this model, huge datasets can be processed in a cloud system. The simulation results show the viruses and trojans are blocked and detected up to 99.95 percent and in continuous 100 h attacks; the blockage ratio of the viruses is 85 percent. The value obtained from the detection and blocking of the virus and trojan is 0.012. The quantity, quickness, and variety for the big data are beneficial in the proposed CCAF. However, this model is limited to verification, encoding, and customer with license access.

In [46], to manage more than one virtual machine (VM) connectivity through a data center, a software stack called industrial technology research institute (ITRI) with security is proposed. In this work, trustable security inside the environment of the cloud is provided. Different modules and components are used to meet security requirements. The system implemented data volume isolation, role-based distributed firewall module, SLA-based traffic shaping, address resolution protocol (ARP) spoofing, and the DDoS to reduce the attacks. Furthermore, web applications' firewall protection, web application firewall (WAF) and lightweight directory access protocol (LDAP), is also used in the system. To provide security to a cloud system using ITRI cloud OS, virtual data center (VDC) isolation, role-based distributed, firewall distributed, WAF protection, and SLA-based distributed shaping are designed, and then implement them inside the cloud system. In VDC isolation first, the media access control layer isolation mechanism is performed which supports the isolation in the multitenant environment. In the second phase, an algorithm is designed, which isolates the volume of the data on VDC. In the role-based distributed firewall, different policies for the security issues are implemented to access control between the networks which in turn protect the VM from high Internet traffic. The proposed work efficiently provides security to the cloud network. The experimental results show, the bandwidth between two virtual machines dynamically shares and is approximately equal to bandwidth allocation.

In [47], the BC technology is used to tackle the security and performance issues in distributed systems. Cloud computing took advantage of the BPDPP services. The functions required for two services assured data derivation and distributed assets. The tamper-proof environment can be achieved by the BC (s) mechanism where the set of authentic minors is used on digital assets to verify the users. Moreover, by using strong cryptography, method block of the transaction is chained together to enable unbeatable records. To achieve vulnerability in BC and provenance in the cloud, the BWH attack is applied in a BC by considering the pool reward mechanism. To add successfully a BC, there is always a need for solving crypto-puzzle in miners which are hard tasks in the computational domain. Therefore, the crypto-puzzle is costly in terms of power and hardware etc.; due to these reasons, the honest miners applied in the pool. A well-known scheme called BWH, in which the malicious pool members joined for truthfully mining block, actually never published any mining blocks before. Hence, the revenue of the attackers in the pool decreases by withholding the valid blocks, but its own reward increases by submitting many shares to the pool manager. The vulnerability in BC cloud arises due to computational power required to obtain the PoW based on consensus; therefore, the BC is implemented on rely PoW to obtain the consensus. The BWH attack occurs in the BC cloud during the pool mining to identify the constraints on the attacker's hashing power to defeat the purpose of pool mining. The simulation results show the attacker's access used more computational power to disrupt the honest mining operation of BC. The strategy of the attackers realizes in two pools where reward schemes are different. The PPLN scheme is useful in keeping the impact lesser of the attackers than the proportional reward scheme.

The trustworthiness parameter of the cloud provider has been improved by using an enhanced QoS-based model in [48]. In this work, the accumulative value of the trust is obtained by updating dynamically the transaction after a specific period. The trust is concluded after analyzing the current status of the transaction. In order to find the user's feedback mechanism as well to find the data credibility, the covariance mathematical technique is used. The best cloud provider has been chosen by the user in this proposed model. For individual cloud service provider, the trustworthiness could be found by lative or computed trust value (ATV). Different SLAs deal with the availability, reliability, data integrity, and turn around efficiency. The SLA parameters include truthfulness, security, and honesty. The resource

Table 10: Integration-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[45]	The multilayered framework proposed is used to integrate and develop the three security technologies; the bioinformatics service can simulate DNA, genes, tumor, and organs of the human body	It ensures the security and safety of all incoming and outgoing data to the cloud; large datasets can be processed on a cloud system and are beneficial for the velocity and volume of the big data	CCAF version 1.1, firewall, identity management, and encryption structured query language (SQL) are used in this model	2016
[46]	This work proposed many modules and algorithms which are implemented at different levels to provide security to the cloud network; different security policies are designed and implemented according to situations	It provides the ability to share the bandwidth efficiently between the two virtual machines	VDC isolation, HTTP, VMs, role-based distributed firewall, and distributed WAF are implemented	2015
[47]	The BC technology used cryptographic enforced distributed ledger system for the security assurance in the cloud; it guarantees the data provenance and the vulnerabilities in the cloud; the BWH attack in BC like the distinct pool reward mechanism	The mechanism used for the security of data is highly strong, and for the attackers, it is difficult to attack because attackers must use extra computational power	The BC technology, BWH, crypto-puzzle, and PoW	2017
[48]	The trustworthiness of the cloud data is the key parameter along with the user credibility feedback; basic assessment model, Qos-based trust assessment, and covariance mathematical models are used to cloud data; the running time, trustworthiness, and user feedback are calculated	The proposed model is best in terms of users' data trustful, confidentiality, and consuming less time	Qos-based trust model, mathematical covariance technique, and basic assessment model are used with cloudSim simulation	2020

availability means users can access the cloud sources at any time. SLA is an agreement between the cloud provider and the user. In short, the basic assessment model, trust assessment model, QoS-based trust assessment model, and covariance mathematical model are used to find out the best cloud provider amongst many and evaluate the credibility of the user's feedback along with the security, reliability, and availability of the data. The cloud Sim platform is used to simulate the best response.

2.9. Security-as-a-Service. Table 11 tells about the references, overviews, techniques used, advantages, and the papers publication years for each research article included in this classification. To build trust in cloud computing is a difficult and complicated task due to the distributed, dynamic, and nontransparent environment. The proposed work trying to win the trust of the users in cloud computing by introducing new methods identifies the fake feedbacks [49]. The one is feedback evaluation and the second is the Bayesian game model. There is a direct relationship between the feedback and trust values, i.e., the attacked feedback has inaccurate value and vice versa. The feedback evaluation model is used to analyze fake feedback. The model indicates the fake feedbacks on the previous average feedbacks. The trust average value increases by rectifying fake feedbacks in comparison with the after fake feedback injection. The task of the feedback evaluation is to identify and rectify fake feedbacks. The malicious users are identified by using the game-theoretic approach. The feedback received by the malicious users is considered as the fake feedbacks and their feedbacks are prevented and not input for the further process to predict the trust. The component evaluates and updates the received feedback from the CSU after receiving service. It qualitatively identifies and rectifies the fake feedbacks. This prevents the circumvention, collusion, latency, and impersonation attacks. The second model called the Bayesian model is used to detect malicious users and prevent their fake feedbacks. A CSU requests the service from a CSP. The game will end if no suitable CSU is found, else the game continues. The trust values of the CSU are calculated using the received feedback. The Bayesian game model is deployed in a fuzzy logic approach. The Bayesian game is between the CSPs and CSUs. Each player has secret information, but it is not shared with any other player. There is no joint comparison between the payoff and cost while the Bayesian model is presented based on cost and payoff. The payoff in a Bayesian model is a qualitative measurement while the cost is a quantitative measurement. The simulation results show the proposed model correctly identifies and rectifies the fake feedback by the feedback evaluation method. The analytical results is matched with the Bayesian model to correctly recognize the malicious users and concluded that the feedbacks received by the malicious users are the fake feedbacks. To prevent the fake feedbacks in a Bayesian model which is due to the strong mathematical model, in this model, a variable delta parameter is used which

Table 11: Security-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[49]	Two new models are proposed to stop the fake feedbacks by the malicious users called the FEBM; the previous feedback average is considered to indicate fake feedback	The variable delta decreases the positive and negative false error with high accuracy	The delta variable factor, the Bayesian game model, and the feedback evaluation	2017
[50]	The attack-defense game-theoretic approach called Stackelberg game is proposed; the players in this game are called the defender and the attacker; the strategies of the defender are open and the attackers follow these strategies; the equilibrium point will be found by the active and passive structured	The Stackelberg model with active and passive structured is used	The attackers achieve the maximum gain of the defender	2018
[51]	In the proposed approach, an integrated solution to cloud security based using the clear framework and the BPMN is discussed; three-layered models are analyzed for the strong security and blocking of threats	The multilayered CCAF security model has 20 percent better performance than the single-layered security models which can block 7348 viruses and trojans; a quick locking system is achieved which can block and quarantine the 9919 trojans and viruses in quick response	The CCAF, BPMN, 10,000 trojans, and 10 PB data in the data center	2016
[52]	The security issues are analyzed on Security-as-a-Service (SecaaS) in this work; a new pattern called leveraging is applied to SaaS; it gives self-managing, automating, and scalable to SaaS	The simulation results show that it outperforms regarding security; the security of the SaaS improves by the cloud-native application	The CNA is used	2017
[53]	The proposed work in this article provided security to a Pr system; the whole work is divided into three steps to provide security to big data; two types of scanning obtained called vulnerability scanning and log scanning which then are correlated to each other to find the attacks on big data	The experimental result shows the attacks count, host computer used, and security tips count to guarantee the speed of analysis	Nikto scanning tools with Nagious and conical correlation are used	2016
[54]	The updated chain VM service proposes to handle the high traffic input to the chain; the halts and deadlock option provide security assurance; the repetition of the previous input data block in new updated chain VM	The technique achieves the increase in the percentage of the security and upgrading and optimizing the security; it configures and runs the desired security stack	Seamless flow, dispatcher VM, and SNAT docker container	2018
[55]	In this model, co-resident attacks encounter instead of looking to the solutions of the attacker after co-locating with their targets; the probability of the attackers co-locating with the targets mitigates in this approach	The cloud Sim and open stack simulators are used which shows the attackers first need to co-locate their VM according to target VM and the attackers achieve hardly up to 40 percent	The virtual machine allocation policy, the PSSP policy, workload balance, and low power consumption	2017
[56]	The approach presents different models to detect and track the already existing threats in the database and new incoming threats to a cloud system	The simulation results show the framework efficiently detects the anomaly security system up to 90%	The signature method, intellectual model, big data technology, and Weka application	2017
[57]	The covert channel analysis performs to secure data at multilevel which enables to secure the data in the presence of unauthorized personnel; different steps follow the data to achieve security	The work protects the data in the presence of an unauthorized person who achieves the trust of users	Covert channel and prototype approach is developed	2015
[58]	The assessment framework proposes to solve a security threat related to the specific client; in this model, different six threats are analyzed, find the concerned client for each threat, and give a secure environment	The model is not fixed to any specific network but can be fitted to any system; the model solves the problem of previously existing assessment framework problems and finds a threat for the concerned client	Spiral network and STRIDE categorizing model is used	2018

decreases the false positive and false negative errors. The feedback trust values distribution is compared in three states called before fake feedback injection, after feedback injection, and after rectification. In short, the Bayesian model is responsible to identify the fake feedbacks with higher accuracy.

The useful decision-maker technique in the attack-defense called the Stackelberg game is proposed in [50]. Two kinds of players are characterized in Stackelberg game called the defender and the attacker. The strategies of the defender are defined in advance and the attacker obeys them. The roles defined for the competitive players called the defender and the attacker is the natural roles. The cloud defender can be a cloud provider or the administrator of the cloud system. The attacker can be any kind of advanced security threats or hackers. The game-theoretic approach gives the tools needed to analyze the behavior and the strategies dependent on payoff functions. The defender wants to minimize the cost during its protection by enhancing the availability of the attacked CI. While on the other hand, the attacker wants to maximize the damages which minimize the cost of the attack itself. The game model formulation includes the player's actions and utility functions. The game structured in two stages: a passive and an active one. By using these two stages, the estimation of the model parameters and the game equilibrium point would be found easily. The equilibrium point can be found by finding the best defense strategy. According to the proposed game model, the defender can rationally choose the right strategy to incorporate the attacks in a proposed way. Besides, the potential cloud attack scenario is modeled between the attackers and the cloud providers as a nonzero-sum SSG. As an output, the attackers achieve a maximum reward which then enhances the defender gain. In short, the proposed game model defines the strategy which maximizes the reward and gain for the attackers and defenders. The empirical analyses prove that, by the security attack management, the attacks prevented the cloud service and data. In this model, a profitable strategy is chosen under a certain attack. The active and passive stages of the SSG provide information about the attacker's behavior.

The CCAF multilayered security model is proposed in [51]. It is believed that the cloud security is only achieved by such an approach that is systematic, adaptable, and well structured. The components, rationale, and overview are explained in the proposed framework to protect the data from different threats. The huge data exist in the data center up to 10 petabytes (PB) which is difficult to protect in real time. The BPMN is used to simulate the data. The CCAF multilayered security is applicable to protect the real time data and consists of three different security layers called the firewall and access control, identity management, intrusion prevention, and, the last but not the least, convergent encryption. A total of 10,000 different trojans and viruses are analyzed in the experiment with two sets of ethical hacking. The proposed CCAF can block the 9,919 viruses and trojans in seconds while the one remaining is isolated or quarantined. The continuous injection of trojans and viruses decrease the blocking percentage of the CCAF, and, in such case, 97.43 percent is quarantined. To make the CCAF more efficient, the BPMN model is combined with the CCAF for the strong security and efficient penetrating testing results. The penetration testing and more other related experiments provided the robustness and precision measurement to the proposed model to justify it from the other approaches. The CCAF multilayer provides multiple protections and a suitable method with the help of which security of the data improves and handles the 10 PB in the data center. The BPMN model is used to understand how the data can be used in rest and motion state within 2 seconds. The time taken by the BPMN to protect the 2 PB is 50 hours; it means an integrated approach is required than the FGSM algorithm and is used for the injection of 10,000 trojans and viruses in the data center. Two different experiments are performed at this stage: one experiment shows the firewall, identity management, and encryption which could block the 54,233,742 and 842 viruses and Trojans, and the remaining 81 could be quarantined. While the other experiment shows the continuous injection of 10,000 trojans and viruses makes the blocking rate decrease from 99.19 to 76.00 percent in 125 hours.

In [52], the authors design a new pattern to improve cloud security. The new design is Security-as-a-Service (SecaaS); it is available just after the SaaS. Leveraging the cloud gives self-managed, automated, and scalable facilities. The developing and deployment of the native design patterns recently appears as an outstanding approach for the application of the clouds. The cloud-native application (CNA) improves the SecaaS. The CNA provides scalability to the cloud system. The experimental results show the better performance in terms of security. However, the design pattern of CNA is complex and has no defined steps for the requirement of detail planning.

In this [53], the authors try to find out an efficient mechanism to provide security to big data on cloud computing. For this purpose, the proposed work divided the design scheme into three main steps. This division includes a vulnerability scan, system log collection, and correlation analysis. This division detects the attacks, illegal approaches, potential threats, and many other security events of the attackers in time based on big data. For vulnerability scan, different tools such as regular using of Nikto and many more are used for the cloud system to carry out the detailed vulnerability scan report for regular network security. The system log collection uses Spelunk, Nagious, and many other tools to collect the detailed system log report. Correlation analysis, also called canonical correlation analysis, is used on the vulnerability and log scanning reports to find out the attacker attacks, corresponding to which the system will issue the warning in time. The cloud computing system has several aspects of security named as to prevent advanced persistent threats, user access control, integrating tools and processes, and real-time data analysis. The experimental results show the system took a total of 136 virtual machines. A Pr is formed by the host machines. The overall cloud system first scans with the help of which a detailed vulnerability scanning report is obtained. This report shows 136 host computers are used, 149 security vulnerability, 178

security warnings, and 497 security tips. After obtaining the vulnerability report in the second step, the system collects the log files for every minute. Then, through conjunction, the vulnerability and log reports are correlated through correlation analysis. The last minute is used to analyze the speed. The log system is used if the suspect is found; then, the log system decides whether this suspicion is an attack or not. The model cannot discover 100 percent attacks of the attacker.

The smooth update service for cloud-based security services is presented in [54]. The virtual machine (VM) executing in a cloud data center receives the network access request by the client on a remote trusted location to a nontrusted remote site and then route it on a chain of security services. The updated facility has by the VM in this approach, in which the VM transfers the network traffic from the initial chain to the updated chain seamlessly and updates the cloud service seamlessly. The halt and the deadlock action is performed on the previous version by the dispatcher VM after confirming the correctness of the updated version. A small test signal flows on the updated chain service to ensure the correctness of the updated chain service. High traffic is input to the updated chain service to analyze the traffic handling operation. The previous stage input data is the block in the updated chain service and checks to ensure that all the input data to the updated chain service are correct and transfer without any problem. The dispatcher VM waits for a specific period after the previous version stops to receive more traffic. The output of a chain VM is input to the next VM in a chain form. The presented work efficiently facilitates in providing the upgrading and optimizing cloud-based security service. The approach mainly performs to configure and can run the desired security stack using a platform called cloud-based security service. The customized and redundant security can be achieved by one or more cloud computing services. The approach efficiently increases the security but with the limitation of scalability issues, lack of customization, and depends on the single point failure. The approach is not limited to one or all the capabilities of firewalls, antivirus, and antimalware. In the experiment, different databases, clients, users, devices, appliances, and cloud-based storage are used and the security results with different ranges are analyzed.

The focus of [55] is on the threat co-resident attack, in which side channels extract the information from virtual machines (VMs) co-located on the same server which are focused. The approach makes many difficulties for the attackers to co-locate with their target by improving the VM allocation policies. The proposed work especially targets the model access attacks by defining security matrices. Then, the matrices of the model notice the difficulties of achieving co-residence under commonly used three policies, after which new policy is designed; this not only minimizes the threat of attacks but also fulfills the requirement of workload balance and power consumption. Then, it practically analyzes these steps by implementing them in cloud Sim and Open Stack simulators. A prototype security policy called PSSF was used earlier. However, the limitation of this prototype is workload balance and power consumption. This work targets these points (workload and power consumption) along with security to achieve high security of the PSSF model, which becomes more applicable in clouds. The MMO techniques are used to improve the PSSF. Firstly, in the proposed work, secure matrices are defined which measures the safety of the allocate policy of the VM which defends against the co-resident attackers. Secondly, these matrices are the model under three basic commonly used VM allocation policies. Thirdly, a new security policy that decreases the probability of the co-locating attackers along with the workload and power consumption is implemented. To avoid obtaining attacker's co-residence, a game-theoretic approach is used which compares three different commonly used VM allocation policies in terms of security, workload, and power consumption. There are two types of VM placements called initial placement and live migration, while the applied model is based on the initial placement. In short, the framework shown before the attackers can extract any private information of the user, and the attacker first needs to co-locate their VM with the target VM. The results show that the simulation was performed on cloudSim and Open Stack; the attackers can achieve the co-resident efficiency hardly up to 40 percent.

An anomaly detection system to secure the cloud environment is discussed in [56]. The wide range of memory is used to store the data in the cloud system which creates many security threats that are uneasy to solve. The cloud computing services have many advantages over the traditional systems, but the cloud systems lack in the concern of security. In the cloud, all the data can be lost due to different security threats and hackers. Therefore, the cloud model needs a data center network that facilitates the model to access a large number of datasets and detects different security threats. Generally, the signature method follows to detect the threats in the cloud model which compare the incoming traffic with the database threats. However, by using this method if a new threat arrives and do not have the database, then it cannot be indicated as a threat. In this scenario, it is more necessary and efficient to use the intellectual method to detect the threats. In the presented model, both the detection systems are added, i.e., intellectual can handle new incoming threats while the signature method used to handle the threats already has by the database. To process the data in a dynamic mode and with speed in big data, different methods and tools are used, i.e., DFS and parallel computing on many servers. They achieve a secure environment, and the proposed model performs different tasks on a cloud system which includes developing secure cloud data center model, developing an anomaly detection system, and big data analysis. The data center model can eliminate the deficiencies of security. The accomplishment becomes possible due to the use of technology architecture, high-speed communications, and unified computing structures. The addition function is added to the data center model for the detection of anomaly secure environments. The Weka application is used which makes the anomaly detection model more secure and accurate. The anomaly methods are mostly used in the area of cloud computing environment, fraud detection in banking, mobile

areas, monitoring of information systems hardware, network's intrusion detection system, processing CCTV images, and suspicious websites. The simulation result shows the developing system provides the high percentage of up to 90 percent of the anomaly detection in the secure cloud environment.

In [57], the covert channel enables to communicate directly the cloud and users in the presence of unauthorized persons while not affecting the data. The protection of data is achieved by multilevel security using the covert channel. The security, feasibility, and performance of the cloud data are achieved by the prototype approach. Different steps involve securing the data while the attackers are present. In this approach, a predefined agreement table is signed between the users and the cloud. An extra fake 8 bits value is generated and transmitted over the wireless channel. The users receive the 8 bits extra value and original data, and the users matched and found out the accurate data according to the agreement able. In this way, the data are secured in the presence of a third party. The simulation result shows the system has acceptance time in cloud data. However, the approach generates extra 8 bits combinations which affect the cloud storage space.

The researchers have worked previously on the assessment approaches for conventional security risk, but they were unable to explicit the concerned risk with respect to a specific attack. In [58], the authors propose such a security model that evaluates the security with respect to a specific threat and having an assessment framework. In this model, the threats which are the concern to the specific client are solved. The risk assessments are mainly divided into three different stages and have a relationship with each other. The three stages of the risk assessment are elicitation, analysis, and control; these all are arranged on a spiral model. The elicitation phase concerns with the assets, vulnerabilities and security requirements, and threat and attack scenarios. The analysis phase is related to the value of assets, the impact, and the relevance of the threats by vulnerabilities. And the last stage but not the least is the controlled phase which describes the management of the vulnerabilities, mitigating risk, and recovery attacks planning. The process of solving threats and concerns with the specific client gives the quantification of security risk. More beneficially, the proposed model can be implemented on any network, and it is not fixed to any one network. The proposed model is called the spiral model and all the stages in this model have a dependency on each other. In this mechanism, the threats for the specific client can be found out and only the concerned client and security are taken into account. The threats are computed in their specific functionalities. All the security risks are taken as a common framework. To categorize the different threats, a model called STRIDE is considered, which has six different threats. The threats are spoofing (S), tampering (T), repudiation (R), information disclosure (I), DoS, and elevation of privilege (E). In short, this model is used for a specific threat which relates to a client that will evaluate to secure the cloud system. The model used has six types of different threats.

2.10. Management-as-a-Service. In order to view the summary of the Management-as-a-service, Table 12 is provided.

In [2], the authors discussed the security issues; they not only concern with inside the network but also relate with the outside of a Pr. As the security of the information is a concern with the third party. Different software scanners are used to ensure the security concern and manage it in a good manner. Three different scanners are used to look after the security of information inside and outside the network. The scanners used for inside the network security management are Metasploit, Nessus, and open VAS. While outside the network security insurance task is performed by using web App tenable IO. In all the network ports, usage information is noticed and a list made for all the ports, that is, which port is used inside or outside the network. Then, according to port (either inside or outside the network), different rules are applied to each port. An Internet protocol identity is provided to a virtual machine through any software tool (Metasploit, Nessus, open VAS, and web app tenable IO). According to experimental results, the Metasploit scanner outperforms than all the other scanners.

In [59], the authors propose the security information and event management (SIEM) architecture to protect the cloud from different intelligent threats. To analyze and recognize the intelligent cyber threats based on virtualization technologies, the SIEM architecture deployed to the Security-as-a-Service platform. The SIEM is an important component of a business platform and network infrastructure which can collect data, aggregate it, normalize it, store it, and correlate the data with the traditional security systems. The traditional systems deployed on the host and network domains are firewall, IDPS, and antimalware systems. The cloud-based service can be protected in several of security events by SIEM architecture. To manage and analyze different log events generated by the cloud security sensors in the security-on-air (SOA) projects, there is a need for SIEM regarding manage log, security events, and correlation analytic by recognizing cyber threats. The data enrichment can be achieved by adding Open SOE and are complemented by adding to the SIEM architecture. The main goal of the SIEM architecture is to provide valuable security and large data correlation to detect cyber threats. The presented model mainly exists by the SIEM engine to collect different data from the users; SIEM storage to store the correlated data, to ensure the security service SIEM user layer is used. The SIEM engine can support the threat analytic and execute it by the virtual machine. The data identifier manager (DIM) is used to recognize the data from various security sensors. The attacker name and traffic information are stored on big data carried out through SIEM baseline and log data frequency. The statistical database uses big data analytics, data mining methodologies by IP address, and the port for data enrichment from collected data and then provides the data in the correlated form to analyze and recognize the cyber threat; these all are achieved by SIEM architecture. The SIEM architecture correlates the collected security features with the aggregate threat datasets. Highly intelligent security performed by the SIEM architecture model on the cloud data.

Table 12: Management-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[2]	The inside and outside security of the Pr network is analyzed here; three different scanners are used to make sure the security inside and outside the cloud; for inside security, Metasploit, Nessus, and open vas tools are used; the outside security of the cloud is performed by web app tenable IO	It secure the data for inside and outside the Pr from hijackers, etc.	The scanners Nessus, Metasploit, open VAS, and web app tenable IO tools are used	2018
[59]	The presented model calculates the baseline values based on day, time, and log data frequency to show out the attacker's name and traffic information; the correlation performs in the model which makes the threat identification easy	The proposed model analyzes and recognizes the cyber threat by obtained correlated information; the SIEM architecture provides the engine to store data and storing the ability to store data	The SOA, OpenSOE, and complemented DIM	2017
[60]	The model presents the security of a cloud system; the quantitative evaluation provided security; the problems of evaluation and comparing the security level offered the presence of complex service supply chain	The presented model provides a well-defined set of security related to the acquired service	Reference evaluation model (REM), SecSLAs algorithms, and complex service supply chain techniques are presented to achieve security goals	2016
[8]	The proposed work ensures the users in the security domain, while they deal in a cloud network; the work enables the users to check and control the data at any stage and level; different models are applied to analyze the security and accountability	It makes the cloud system according to the demand of the users who can check and control their data at any stage	The PM in the cloud, RSASS system, data security model, and CIA models are used	2015
[61]	Various old policies of the cloud network security are compared with network security; besides, some additional new knowledge-based policies are added to cloud security, and then experimentally analyze and find the correctness and effectiveness of the proposed work	The experimental results proved the design policies stood well to old policies for cloud security	A multidimensional integer space conflict detection algorithm is proposed	2016
[62]	According to the job of the user and computer security provided to the cloud system in this framework, through GA-based job security, two new concepts are achieved in this work called security on demand and improved trust level	By using the algorithms and techniques in this work, the simulation results show the high-level security with the minimum cost of time	The GA-based job security technique is used	2015
[63]	Two security threats called timing attacks and DoS are analyzed and secure the cloud system from these threats; the security-aware and NDTMSI with the agent-based monitoring system is proposed	The proposed approach provides magnificence security without substantial modification and provides integrity and confidential and authentication monitoring to the cloud	The safe random number generator (BBS), secure generic scheduler, nondeterministic model, a secure hashing algorithm (SHA) scoring workers, security bias model, and leveraging genetic heuristic approach	2017
[64]	The hybrid cryptographic system (HCS) is applied to the cloud system to secure the data; in this work, symmetric and asymmetric approaches are analyzed to encrypt and decrypt the data	In this work, the system from start to end is secure which achieves the trust of the users until the data stores on the cloud	In the hybrid cryptographic system, asymmetry data encryption RSA and symmetry data encryption AES are applied	2017

The per-service SecSLA discusses in [60]. The authors show the provider and consumer reach an agreement point on the features of the security of each service instead of leased. In this framework, each customer fixed a different security level agreement (SLA) for each leased service. A well-defined set of security rules guarantees the acquire service with respect to providers. The reference evaluation model (REM) provides a quantitative level of security. In the presence of a complex service supply chain, the security offered by cloud providers involving resource acquisition from different CSPs. In this model to build up per-service security, SLA starts from currently available public repositories called STAR repository. The security control by the providers is used to fill a declarative section of respective security SLA; it identifies the security features provided by the CSPs. Subsequently, the combined security SLA is built by generating an enhanced consensus assessment initiative questionnaire (CAIQ) in the availability of a complex supply chain. The SLA can monitor the additional security capabilities introduced in the supply chain, and the security SLAs are compared to the REM technology. In short, the combined per-service security SLA is currently obtained by simply putting all together with the controls declared by the CSPs in the supply chain. The model outperforms in terms of security.

In [8], the authors describe the importance of security and accountability in cloud computing using different models. The researchers focus on security availability and performance. The top issue is security, and it is still important in the cloud, as the users have no control in the security section. All the security actions, planes, and policies on data are implemented by the CSP and the users have no interference. The modification and deletion of the data are performed by the users; in this case, the service provider must maintain the sequence and order of the data as data have previously. The role of the distributed protocol is important as the data is stored at different places due to which latency is generated. Accountability is another parameter in the cloud which ensures the users about the security of the data. Accountability enables the user to check security, transparency, and control. It brings the confidence; the user can control, check, and verify data at any stage according to its expectation. The log recorder uses to check and analyze the actions taken by the users are suitable or not. Accountability builds the trust of users on the CSP. Different models are used to ensure security and accountability in the cloud: PM in cloud, RSASS system, data security model, and cloud information accountability framework. After implementing all these models on data, the results show for the security purpose the best models are data security model, PM, and CIA framework. For accountability, the outperformed model is cloud information accountability (CIA) and the RSASS system. Overall, the CIA model is best for both (security and accountability). The main drawback of the CIA model is its larger size.

In [61], different old policies are discussed and then the new policies are presented for cloud security. In this work, the policy and knowledge-based comparison are made between cloud security and network security. A multidimensional space and sum up of a conflict detection method are proposed for cloud security policy, in which mapping of the security field to an integer multidimensional space set is according to the condition of field mapping principle. The experimental results are carried out through different central processing units (CPUs), which find the correctness and effectiveness of security policy collision detection algorithm on multidimensional integer space. The result shows the time computational of the proposed policies when the experiments are repeatedly carried out. However, due to the time dynamic of the proposed work this model is not stable in the time domain.

The job security problem of the cloud security is proposed in [62]. The proposed work divided the whole cloud system into four architecture-based layers called SOA architecture, management middle-ware, resource virtualization, and physical resource. The chromosomes and genes are used to functionalize the algorithm and are called GA-based job security. In this algorithm, each chromosome is utilized to show the schedule of a set of jobs on many computers. The gene is used to show the relation between jobs and computers. Many users and computers are considered in which each user has a task which is input to the computer; the proposed algorithm then analyzes the security level according to the job of a computer. In summary, two new concepts are analyzed in this framework called security demand, to improve the trust level of the users. The simulation result proves that the proposed framework provides a high level of security to a cloud system by consuming minimum time.

The DoS and timing attack prevention are the computational cloud challenges and presented in [63]. A novel architectural model is based on a multiagent scheme and security-aware nondeterministic metascheduler driven by genetic heuristic to enforce the cloud security. The proposed approaches prevent the cloud system from the DoS and timing attacks in an Open Stack platform. The basic security objectives in modern clouds are the preservation of confidentiality, integrity, and availability. The proposed work incorporates the first two issues in this article. The information security methods are used for the cryptography service designed and implemented for the theoretical model. To solve the above proposed security issues, the cloud architecture divided into multiple components to secure the whole cloud system. Amongst the total eighteen security control points, the proposed work encounters the access control, protection, audit and accountability planning, security assessment and authorization, risk assessment, identification and authentication, system and communication protection, incident response and system, and the last information integrity. The proposed model is like the resource management system; it supports the inside secureness of the CI by task distribution according to required security demands coming from the cloud consumers. To meet this security option, the batch scheduler leveraging a genetic heuristic approach is used. To monitor the task flow, characterizing the scheduled processing supports the multiagent system in cloud computing. By doing such security operation, the model is protected by DoS and timing attacks. The scheduling, monitoring, and reporting activities are

carried out in nondeterministic time intervals. Two additional models to secure the model more are proposed. One is called scoring worker model and the other one is called security bias. The scoring worker model states the virtual machines are used for the scheduling tasks only and are characterized by the security level at least equal to or higher than the demands of customers. The averaged time associated with security operation processing is added to the fee for the total runtime for each customer. Second, the security bias model considered the cryptographic operations associated with each task. The enlarging of time required for the task processing in a scheduling process is modeled in security bias. In short, the simulation results show the proposed model effectively increase safety without substantial modification. The model is dynamic and used for different schedule types. This property of the model ensures proper security. The elements which are incorporated in scheduling are a denial of service (DoS) and task injection prevention and integrity monitoring and authenticity checking with a standard.

The CSPs increase their demands day by day, but the security of the data in the cloud is still a question mark. In [64], the authors propose an ecosystem in which different techniques are applied to secure the data. Many researchers propose different algorithms and techniques; most of them concern with specific threats. However, the proposed framework designs such techniques and algorithms which secure the whole system from the start to end. The hybrid cryptographic system (HCS) is analyzed in the proposed task. The focus of the work is in the encryption and decryption of the data efficiently. The cloud environment is secured by analyzing HCS for the symmetric and asymmetric encryption. The rehabilitation services administration (RSA) and AES algorithms are used to perform symmetric and asymmetric operations to secure the whole system until the end. The RSA algorithm generates the keys privately and publicly which are later used for the encryption. Different parameters should be noticed while analyzing the user data which are data protection, traffic hijacking, isolation of resources, and malicious insider. The hashing and salting techniques are also applied to the ecosystem to strengthen the encryption process at different stages. The proposed framework outperforms to secure the whole system. This achieves the trust of the users, and the data are secure until it stores on the cloud.

2.11. Testing-as-a-Service. To minimize the time consumption for the researchers the whole summary of this classification component is presented in Table 13.

In [10], the authors analyze and test the security issues of an online education system. The security issues are highly important to secure the data of a system. The online education system is mostly popular nowadays; therefore, hackers and attackers may want to expose and leak the data. The data store in the cloud is not in the control of the user. The App Scan tool is used to analyze and test the security of the education system. The main working principle of App scan: first, it finds the web with the help of which the directories and site parameters can be analyzed regarding security. Second, a modified HTTP tool is used to check the attempt attacks on the data on the basis of which rules and arrangements are implemented by the security responsible authority. At last, it tests the overall education network by the load-runner tool. According to experimental results, high risk issues are analyzed and resolved through app scanner after resolving no higher-level and middle-level risks exist.

In [65], the MapReduce framework for cloud computing is provided. The MapReduce currently is the most popular and dominant programming model. Therefore, it is essential to protect the probity of the data processing of the MapReduce model. The malicious workers are categorized into collusive and noncollusive; the workers try to degrade the results to find the easiest way to attack cloud computing. The important task is to find out malicious workers in an efficient manner. In the proposed framework, security protection is designed to find the malicious workers. The proposed security system consists of two mechanisms called credit-based replicate tasks and verification which can be combined to behave efficiently. The integrity in the map phase of the MapReduce is obtained in this work. MapReduce is a programming model and generates large datasets. The jobs of the users are submitted to a scheduling machine. The input datasets are broken into small independent pieces from 16 to 64 MB in size by the MapReduce model. Then, the chunks are managed by the map task in a parallel way. The outputs are sort by the proposed map which then inputs to reduce the tasks. Both input and output jobs are stored in DFS. The proposed MapReduce is divided into two phases: one phase is the map phase and the second is the reduce phase. The workers in the map and reduce phases are called the mappers and reducers, respectively. In the map phase, the input datasets are divided into small chunks. And in the reduce phase, the intermediate results are distributed to the reducers to reduce the task associated with reducers. When the reducers receive a reduce task, then they wait for the notification about the map task completion and then receive intermediate results as their inputs. After this, the reducers input their data to FDS and then the reducers notify the master that they return the results to the user job. To detect the malicious workers the framework consists of the replicate task and verification approach. When the task queue picked by the master, it will be forwarded to any two workers. The two workers execute this task which is called the replicate task. By obtaining the two results from the two workers, the master compares these results if they are different; then, it means one of the workers is a noncollusive worker. To detect which one worker is noncollusive, the improved replicate task which is a credit-based replicate task is proposed. The simulation results enable the users to detect all the collusive workers with different malicious ratio. When the quiz threshold is set to 6 the overhead of the proposed model was no longer than 2.5, even the malicious ratio equals 0.5. The response time is almost 3 percent longer than the traditional models. In short, high security with malicious workers is obtained for cloud computing which is a sign of stable and efficient.

Table 13: Testing-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[10]	The online education system is made secure in this work; however, different attackers and hijackers want to leak and expose the data; the App Scan tool is used to make secure and analyze the data; however, a modified HTTP tool is used to find the attempt attacks	In this work, the security of the cloud is arranged according to attempt attacks	App Scan and modified HTTP are used	2018
[65]	The novel approach called MapReduce is the programming model which is presented; the big datasets are divided into small pieces and then input to the scheduling machine; the whole framework is divided into two phases called map and reduce phases	The overhead mechanism is almost eliminated with high accuracy and in an efficient manner	The MapReduce programming model, malicious workers (collusive and noncollusive), protection framework, credit-based replicate tasks, and verification	2016
[66]	The optimal decryption method has been proposed to encrypt cloud data; the RRA-CPA-based PKE has been improved to avoid random attacks on the cloud data	This model presents the optimal result in terms of avoiding the random attacks on cloud data along with the strong decryption	IND-CCA secure PKE scheme and RRA-CPA-based PKA scheme have been presented	2020

In [66], the different random attacks on the data encryption techniques have been discussed. The encryption techniques include RRA-CPA and have optimal decryption algorithms. In the PKE scheme to avoid random attacks, an improved version has been discussed of the PKE scheme which encounters the different random attacks. For the purpose of encryption, the information, firstly, the hardcore function has been applied to gain the output; then efficient decryption and cipher text size have been applied to this encryption. This proposed model efficiently enhances the decryption.

2.12. Infrastructure-as-a-Service. Table 14 explains the short summary of the Infrastructure-as-a-Service.

In [67], the software-defined network (SDN) and information-centric networking (ICN) are analyzed in a cloud model. The purpose is to put both SDN and ICN in a cloud and to ensure the security of the data. With the help of these flexible infrastructures and stable networks, performance is achieved in the cloud environment as per service level agreement. The ICN is considered the building block of the proposed framework because of the following reasons: the architecture related to ICN is more efficient than the IP-based networking and the host-oriented communication model by default replaces to a content centric model. The information is accessed by the identifier rather than the host in the ICN, whereas the SDN decouples the control plane in an efficient manner which is responsible to make decisions to route a packet and processing of the packet to the desired destination. This property of the SDN administrates the network to provide services of routing, policy enforcement, and the last security. The proposed framework provides autoconfiguration to topology and policy of the network so that a user faster avails the cloud service. Through the naming manager, the data is given to each user in the proposed framework, which ensures the integrity of the security.

The security system of the enterprise is proposed in [68]. Infrastructure construction is needed to combine the information security establishment. The Pr network security is methodical, and there is a chance of damaging the network. The big data security and basic network security condition consider the Pr network security as an arrival point. Then, they analyze the relevant evaluation indexes and establish the evaluation system model along with the key technologies in cloud enterprises. The artificial intelligence provides some new possibilities to solve the problems of network security such as complex security data, lack of real time, feasible information, and professional protection technology. The construction system and information security management system are the supplement to each other. The core of enterprise information security is the security management strategy which was implemented perfectly and strictly. Only network security that has improved the speed of information construction people can enjoy the ease of network safety. The key technology for the Pr is divided into five different layers called device security, network security, system security, and application security and data security layers. By analyzing the threats on each layer and then performing a positive action according to threat gives us a secure, confidentially, integrity, and controllability network.

In [69], the authors presented different security issues and their suitable solutions. The proposed work categorizes cloud computing into two sections called the deployment model and service delivery model. The deployment model includes public, private, hybrid, and community clouds, while the service delivery model includes SaaS, PaaS, and IaaS. Providing the security and reliability to the cloud environment is the responsibility

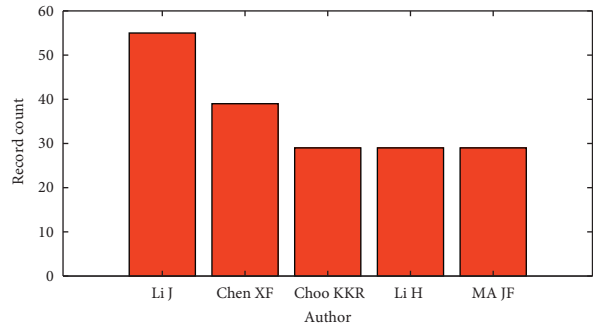

Figure 4: Author-based Survey.

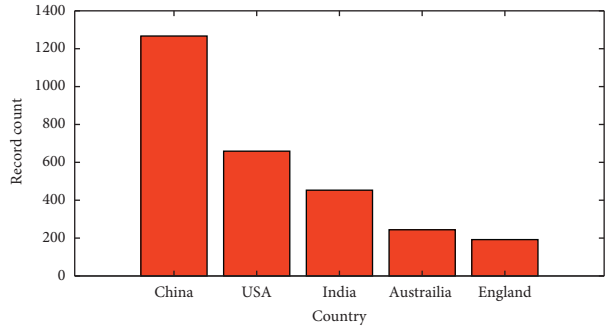

Figure 5: Country-based Survey.

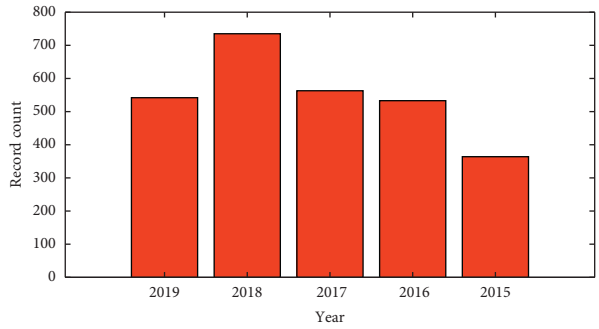

Figure 6: Year-based Survey.

of both user and cloud providers. The security issues and their corresponding solutions are presented in this article. The multitenant architecture problems are overcome through isolation and segmentation techniques. The perishing attacks and other breach threats are overcome through web browsers. Through service level agreement, the problems of the maintenance of the QoS, data loss, and other threats are solved. Using strong two-factor authentication techniques, the problems of account hijacking and related threats are solved. The DoS attack and the abuse of cloud service are prevented by using a honeypot system. In this article, different attacks are mentioned through CSA which are the topmost nine (09) attacks on the cloud system until 2013: data breaches, data loss, account hijacking, insecure APIs, DoS, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology issues.

The control blockchain-based framework called the Auth-Privacy chain is adopted to minimize the leakage and temper the data in the cloud [70]. First, the identity is provided to a node and this address is stored in blockchain; then, according to this address encryption is made. The process is called access control authorization and authorization revocation in the Auth-privacy chain. Along with these enterprises, the operating system is also implemented. After applying all these frameworks, the outcomes show that the proposed work not only minimizes the hackers and administration from illegal accessing but also provides protection to authorized privacy. Besides this, the Auth-privacy chain is responsible to provide integrity, confidentiality, and accountability along with the protection from many inside and outside unauthentic attacks. Blockchain is an open plain temper proof such as a distributed database. In DO command, a user can upload the data in the cloud, while

Table 14: Infrastructure-as-a-Service.

References	Overviews	Advantages	Techniques	Years
[67]	Two networks called software-defined network (SDN) and information-centric networking (ICN) are analyzed on the cloud model to secure the data; the ICN is considered the building block of the framework, and SDN decouples the control plane	This flexible infrastructure highly provides data security	Software defines network, and information-centric networking are applied	2017
[68]	The private network analyzes the big data to secure the enterprises; different threats on different layers are analyzed and give a solution to each threat; by doing this a secure enterprise Pr network is achieved	The framework gives different solutions for the different threats on five layers, and the Pr becomes more secure and confidential	The big data, key technology, five layers, and antivirus technology	2018
[69]	The cloud providers and the users both are responsible to deliver reliable and secure data over the cloud; different security threats and their solutions are analyzed here; the CSP protects the sharing of technology issues; the security provided is architecture and layer base	Highly secure techniques are discussed which fully protects the data on any deployment model	Isolation and segmentation, web browser, service level agreement, two-factor authentication, and many more techniques are used	2016
[70]	The leakage and temper of the cloud data is minimized; along with these, the privacy and unauthentic scenarios are being analyzed using a framework called the Auth-privacy chain, a blockchain framework, and enterprise operating system	This proposed framework eliminates the data leakage and temper of data in the cloud system and provides privacy	Blockchain-based access control, the Auth-privacy chain, and enterprise operating system	2020

DU command is responsible for accessing the data if the cloud allows. Cloud is a semitrusted platform, and in this framework, blockchain is assumed trustful. DO command uploads the data or resources to the cloud, and DU command sends a request to the cloud; then, the cloud checks whether blockchain has premium, and hence, finally replies according to the response.

3. Conclusion

In this survey, different challenges are highlighted for cloud computing security based on cloud components. These challenges are related to the outside as well as inside the cloud systems. Several techniques, approaches, models, algorithms etc., are applied at different levels to cloud components to make sure the security of the cloud models. In this paper, the classifications are made in which different issues related to security are solved with different techniques. The classifications involve the overviews of the proposed schemes in which specific issues related to cloud security are analyzed; their advantages and the techniques used to solve the concern issues are discussed. On the basis of cloud component classification, the researcher can pick out the desired technique related to the concern security issue while dealing with cloud security. Bibliometric survey based on authors, countries, and years has been conducted in the field of cloud computing security as can be seen in Figures 4–6, respectively. The bar graph of this survey shows the authors, countries, and years with their record in the field of cloud computing security. Moreover, the future directions are given which are concluded after analyzing all the problems in cloud security components which are to be improved yet. Table 1 shows the acronyms used in this manuscript.

4. Future Directions

The future directions for cloud computing security are

(i) The signature method is used to capture a specific threat and not allow the threats to interfere with the cloud data. This method accurately focused on the specific threat with a lower false rate. However, the signature method recognizes only threats that are known to its directory; this is unable to recognize the unknown threats. In the future, this method can be improved to catch all kinds of threats.

(ii) The cloud-native application pattern is used for cloud data security purpose. However, designing the cloud-native application (CNA) pattern is a complex procedure that required detailed planning and has no defined steps. Therefore, in future work, the researchers can optimize this technique.

(iii) The advanced encryption standard technique is mostly used to encrypt the data which provides strong security against the attackers. However, the AES does not withstand the brute force attack and

linear cryptographic analysis. This is a common kind of threat which is mostly occurring and not handled by the AES. In future work, AES needs to modify for the brute force threat.

(iv) The security service level agreement algorithms have been proposed to make secure the cloud data. Different techniques in this approach are used to evaluate security issues such as reference evaluation model and complex service supply chain techniques. However, in these techniques, the security evaluation for the cloud is not concerned with the end-to-end domain. Furthermore, the techniques considered in this approach generate the extra 8 bits attachment which affects the cloud storage space. Therefore, in the future, researchers can improve these techniques according to need.

(v) The virtual machines (VMs) efficiently enhance the cloud security, but it fails in scalability issues and depends on the single point failure and lack of customization. Therefore, in future work, these issues can be fixed and improve.

(vi) Most of the traditional algorithms are applied to secure the cloud systems at different stages and levels such as data encryption standard, advanced encryption standard, and Rivest–Shamir–Adleman cryptosystem, which are not automated. The future challenge is to make them in an automatic form which will enhance the accuracy and reduces the time consumption.

(vii) Different software, tools, and cryptographic approaches are analyzed to secure the cloud storage and layers, but these techniques are complex and more time consuming. In future work, these techniques can be converted to a noncomplex process, which consumes minimum time.

(viii) The App scan tool is used to secure the cloud data, but it is unable to stop all the threats. It can miss those threats and allow entering the cloud data which are unknown to its directory. In future, the researchers can expand and increase the domain of the App scan tool in terms of the directory which can capture and remove all the threats.

(ix) For the Big data, technology-based tools (Map-Reduce etc) are used to secure the large structure or unstructured data. Such traditional software cannot handle the massive data which results in the poor security of the big data. To overcome such an issue the researchers should design the optimal software tools that are best in their performances.

(x) A load balancing technique is used to ensure the security resources and performances used on it. While, it is also used to avoid data overloading and underloading in virtual machines which itself is a big challenge. The researchers should minimize the overloading and under loading of the data in the future and should maintain an intermediate data bunch to overcome this problem.

Data Availability

The data used to support the findings of the study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project number RSP-2020/184 and partially supported by the Faculty of Computer Science and Information Technology, University of Malaya under Postgraduate Research Grant (PG035-2016A).

References

[1] A. Tahir, F. Chen, H. U. Khan et al., "A systematic review on cloud storage mechanisms concerning e-healthcare systems," *Sensors*, vol. 20, no. 18, p. 5392, 2020.

[2] S. Narula and A. Jain, "Cloud computing security: Amazon web service," in *Proceedings of the 2015 Fifth International Conference on Advanced Computing & Communication Technologies*, pp. 501–505, Rohtak, Haryana, India, Feburary 2015.

[3] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[4] I. Gordin, A. Graur, A. Potorac, and D. Balan, "Security assessment of OpenStack cloud using outside and inside software tools," in *Proceedings of the 2018 International Conference on Development and Application Systems (DAS)*, pp. 170–174, Suceava, Romania, May 2018.

[5] R. Aluvalu and L. Muddana, "A survey on access control models in cloud computing," *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India (CSI)*, , 2015.

[6] C. Feng, A. Muhammad, A. Ahmad, A. Ullah, and H. U. Khan, "Towards energy-efficient framework for IoT big data healthcare solutions," *Scientific Programming*, vol. 2020, Article ID 7063681, , 2020.

[7] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: a cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[8] I. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: a survey," *Computers*, vol. 3, no. 1, pp. 1–35, 2014 Mar.

[9] M. Iglesias-Urkia, A. Orive, A. Urbieta, and D. Casado-Mansilla, "Analysis of CoAP implementations for industrial internet of Things: a survey," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 7, pp. 2505–2518, 2019.

[10] K. El Makkaoui, A. Ezzati, A. Beni-Hssane, and C. Motamed, "Cloud security and privacy model for providing secure cloud services," in *Proceedings of the 2016 2nd International*

Conference on Cloud Computing Technologies and Applications (Cloud Tech), pp. 81–86, Marrakech, Morocco, May 2016.

[11] G. Beier, S. Niehoff, and B. Xue, "More sustainability in Industry through industrial Internet of Things?" *Applied Sciences*, vol. 8, no. 2, p. 219, 2018.

[12] A. Singh and K. Chatterjee, "Cloud security issues and challenges: a survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[13] G. L. Reddy and B. M. Krishna, "Survey of cloud computing and its application," *Journal Impact Factor*, vol. 3, p. 24, 2018.

[14] X. Sun, "Critical security issues in cloud computing: a survey," in *Proceedings of the 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing,(HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 216–221, Omaha, NE, USA, May 2018.

[15] R. Kaur and J. Kaur, "Cloud computing security issues and its solution: a review," in *Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, New Delhi, India, pp. 1198–1200, March 2015.

[16] N. C. Paxton, "Cloud security: a review of current issues and proposed solutions," in *Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pp. 452–455, Pittsburgh, PA, USA, November 2016.

[17] W. Dashti, A. Qureshi, A. Jahangeer, and A. Zafar, "Security challenges over cloud environment from service provider prospective," *Cloud Computing and Data Science*, vol. 1, no. 1, pp. 12–20, 2020.

[18] D. M. Vistro, A. U. Rehman, M. S. Farooq, A. Abid, and M. Idrees, "A survey ON the role OF security and integrity issues IN cloud," *Journal of Critical Reviews*, vol. 7, pp. 1456–1469, 2020.

[19] J. B. Hong, A. Nhlabatsi, D. S. Kim, N. A. Hussein, and K. M. Khan, "Systematic identification of threats in the cloud: a survey," *Computer Networks*, vol. 150, pp. 46–69, 2019.

[20] M. Anisetti, C. A. Ardagna, E. Damiani, and F. Gaudenzi, "A security benchmark for openstack," in *Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, pp. 294–301, Honolulu, HI, USA, June 2017.

[21] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pp. 458–467, Madrid, Spain, May 2017.

[22] O. V. Lindqvist, G. Fitzgerald, Z. Wu, Y. Wu, F. Shen, and X. Luo, "Osmotic interrelationship between blood and gut fluid in the isopod Porcellio scaber Latr. (Crustacea)," in *Proceedings of the 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 57–59, Shanghai, China, June 2018.

[23] U. Ghosh, P. Chatterjee, D. Tosh, S. Shetty, K. Xiong, and C. Kamhoua, "An SDN based framework for guaranteeing security and performance in information-centric cloud networks," in *Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, pp. 749–752, Honolulu, HI, USA, June 2017.

[24] S. Siadat, A. M. Rahmani, and H. Navid, "Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model," *The Journal of Supercomputing*, vol. 73, no. 6, pp. 2682–2704, 2017.

[25] A. Jakóbik, D. Grzonka, and F. Palmieri, "Non-deterministic security driven meta scheduler for distributed cloud organizations," *Simulation Modelling Practice and Theory*, vol. 76, pp. 67–81, 2017.

[26] Y. Wu, Y. Lyu, and Y. Shi, "Cloud storage security assessment through equilibrium analysis," *Tsinghua Science and Technology*, vol. 24, no. 6, pp. 738–749, 2019.

[27] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 457–471, 2015.

[28] F. Kong, Y. Zhou, B. Xia, L. Pan, and L. Zhu, "A security reputation model for IoT health data using S-AlexNet and dynamic game theory in cloud computing environment," *IEEE Access*, vol. 7, pp. 161822–161830, 2019.

[29] R. Y. Chou, G. W. Bannister, and inventors, "Nubeva Inc, assignee. Seamless service updates for cloud-based security services," United States Patent US 10,530,815, 2020.

[30] F. R. Martinez and E. Pulier, "Csc Agility Platform Inc, assignee. System and method for a cloud computing abstraction layer with security zone facilities," United States Patent Application US 16/058,688, 2019.

[31] S. Kang, B. Veeravalli, and K. M. Aung, "A security-aware data placement mechanism for big data cloud storage systems," in *Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 327–332, New York, NY, USA, April 2016.

[32] J.-H. Lee, S. K. Young, H. K. Jong, and K. K. Ik, "Toward the SIEM ar-chitecture for cloud-based security services," in *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 398-399, Las Vegas, NV, USA, October 2017.

[33] Y. Han, J. Chan, T. Alpcan, and C. Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 1, pp. 95–108, 2015.

[34] A. De Benedictis, V. Casola, M. Rak, and U. Villano, "Cloud security: from per-provider to per-service security slas," in *Proceedings of the 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pp. 469–474, Ostrava, Czech Republic, September 2016.

[35] V. Chang and M. Ramachandran, "Towards achieving data security with the cloud computing adoption framework," *IEEE Transactions on Services Computing*, vol. 9, no. 1, pp. 138–151, 2015.

[36] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: a security framework for business clouds," *Future Generation Computer Systems*, vol. 57, pp. 24–41, 2016.

[37] H. Cheng, C. Rong, K. Hwang, W. Wang, and Y. Li, "Secure big data storage and sharing scheme for cloud tenants," *China Communications*, vol. 12, no. 6, pp. 106–115, 2015.

[38] Z. Li, J. Ge, H. Yang et al., "A security and cost aware scheduling algorithm for heterogeneous tasks of scientific workflow in clouds," *Future Generation Computer Systems*, vol. 65, pp. 140–152, 2016.

[39] Z. Hu, S. Gnatyuk, O. Koval, V. Gnatyuk, and S. Bondarovets, "Anomaly detection system in secure cloud computing environment," *International Journal of Computer Network and Information Security*, vol. 9, no. 4, p. 10, 2017.

[40] J. Agarkhed and R. Ashalatha, "An efficient auditing scheme for data storage security in cloud," in *Proceedings of the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, pp. 1–5, Delhi, India, April 2017.

[41] A. Nhlabatsi, J. B. Hong, D. S. Kim, R. Fernandez, N. Fetais, and K. M. Khan, "SpiralŜRA: a threat-specific security risk assessment framework for the cloud," in *Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pp. 367–374, Lisbon, Portugal, July 2018.

[42] P. Y. Wang and M. Q. Hong, "A secure management scheme designed in cloud. In2016 IEEE 2nd International conference on big data security on cloud (BigDataSecurity)," in *Proceedings of the IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 158–162, New York, NY, USA, April 2016.

[43] S. A. Hande and S. B. Mane, "An analysis on data Accountability and Security in cloud," in *Proceedings of the 2015 International Conference on Industrial Instrumentation and Control (ICIC)*, pp. 713–717, Pune, India, May 2015.

[44] J. Xu, C. Liang, H. K. Jain, and D. Gu, "Openness and security in cloud computing services: assessment methods and investment strategies analysis," *IEEE Access*, vol. 7, pp. 29038–29050, 2019.

[45] J. H. Lee, Y. S. Kim, J. H. Kim, and I. K. Kim, "Toward the SIEM architecture for cloud-based security services," in *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 398-399, Las Vegas, NV, USA, October 2017.

[46] T. S. Fatayer and K. A. Timraz, "MLSCPC: multi-level security using covert channel to achieve privacy through cloud computing," in *Proceedings of the 2015 World Symposium on Computer Networks and Information Security (WSCNIS)*, pp. 1–6, Hammamet, Tunisia, September 2015.

[47] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[48] H. Hassan, A. I. El-Desouky, A. Ibrahim, E.-S. M. El-Kenawy, and R. Arnous, "Enhanced QoS-based model for trust assessment in cloud computing environment," *IEEE Access*, vol. 8, pp. 43752–43763, 2020.

[49] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust—a security assessment model for infrastructure as a service (IaaS) clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 523–536, 2015.

[50] N. S. Darwazeh, R. S. Al-Qassas, and F. AlDosari, "A secure cloud computing model based on data classification," *Procedia Computer Science*, vol. 52, pp. 1153–1158, 2015.

[51] H. Cui, Y. Li, X. Liu, N. Ansari, and Y. Liu, "Cloud service reliability modelling and optimal task scheduling," *Iet Communications*, vol. 11, no. 2, pp. 161–167, 2017.

[52] S. Feng, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, "Joint pricing and security investment for cloud-insurance: a security interdependency perspective," in *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Marrakech, Morocco, April 2018.

[53] D. H. Sharma, C. A. Dhote, and M. M. Potey, "Implementing intrusion management as security-as-a-service from cloud," in *Proceedings of the 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, pp. 363–366, Bengaluru, India, October 2016.

[54] M. Usman, M. Ahmad Jan, and X. He, "Cryptography-based secure data storage and sharing using HEVC and public clouds," *Information Sciences*, vol. 387, pp. 90–102, 2017.

[55] M. Ramachandran and V. Chang, "Towards performance evaluation of cloud service providers for cloud data security," *International Journal of Information Management*, vol. 36, no. 4, pp. 618–625, 2016.

[56] K. K. Gola, R. Rathore, and S. Rastogi, "Secure: dynamic distributed load balancing technique in cloud computing," *International Journal of Advanced Research in Computer Science*, vol. 9, no. 1, 2018.

[57] A. Arora, A. Khanna, A. Rastogi, and A. Agarwal, "Cloud security ecosystem for data security and privacy," in *Proceedings of the 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence*, pp. 288–292, Noida, India, January 2017.

[58] D. Zhe, W. Qinghong, S. Naizheng, and Z. Yuhan, "Study on data security policy based on cloud storage," in *Proceedings of the 2017 IEEE 3rd International Conference on Big Data Security on Cloud (Bigdatasecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 145–149, Beijing, China, May 2017.

[59] C. Prakash and S. Dasgupta, "Cloud computing security analysis: challenges and possible solutions," in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 54–57, Chennai, India, March 2016.

[60] G. Ducatel, J. Daniel, T. Dimitrakos, F. El-Moussa, R. Rowlingson, and A. Sajjad, "Managed security service distribution model," in *Proceedings of the 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS)*, pp. 404–408, Beijing, China, August 2016.

[61] M. Derfouf, A. Mimouni, and M. Eleuldj, "Vulnerabilities and storage security in cloud computing," in *Proceedings of the 2015 International Conference on Cloud Technologies and Applications (Cloud Tech)*, pp. 1–5, Marrakesh, Morocco, June 2015.

[62] T. C. Chiueh, E. J. Chang, R. Huang, H. Lee, V. Sung, and M. H. Chiang, "Security considerations in ITRI cloud OS," in *Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST)*, pp. 107–112, Taipei, Taiwan, September 2015.

[63] W. Zhu and C. Lee, "A security protection framework for cloud computing," *JIPS*, vol. 12, no. 3, pp. 538–547, 2016.

[64] B. H. Lee, E. K. Dewi, and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," in *Proceedings of the 2018 27th Wireless and Optical Communication Conference (WOCC)*, pp. 1–5, Hualien, Taiwan, April 2018.

[65] L. Qing, Z. Boyu, W. Jinhua, and L. Qinqian, "Research on key technology of network security situation awareness of private cloud in enterprises," in *Proceedings of the 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pp. 462–466, Chengdu, China, April 2018.

[66] P. Liu, "Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/edge computing," *IEEE Access*, vol. 8, pp. 16750–16759, 2020.

[67] K. A. Torkura, M. I. Sukmana, F. Cheng, and C. Meinel, "Leveraging cloud native design patterns for security-as-a-service applications," in *Proceedings of the 2017 IEEE*

International Conference on Smart Cloud (Smart Cloud), vol. 3, pp. 90–97, New York, NY, USA, November 2017.

[68] H. Li, R. Lu, J. Misic, and M. Mahmoud, "Security and privacy of connected vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 4–6, 2018.

[69] H. Zhang, "Research on job security scheduling strategy in cloud computing model," in *Proceedings of the 2015 International Conference on Intelligent Transportation, Big Data and Smart City*, pp. 649–652, Halong Bay, Vietnam, December 2015.

[70] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: a blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.