

SECURITY ISSUES IN CLOUD COMPUTING USING EDGE COMPUTING AND BLOCKCHAIN: THREAT, MITIGATION, AND FUTURE TRENDS - A SYSTEMATIC LITERATURE REVIEW

Muzammil Ahmad Khan ^{1,2*}, Shariq Mehmood Khan ² and Siva Kumar Subramaniam ³

¹ Department of Computer Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan;

² Department of Computer Science and Information Technology, NED University of Engineering and Technology, Karachi, Pakistan

³ Faculty of Electronics and Computer Engineering, Universiti Teknikal Malaysia, Melaka, Malaysia

Email: muzammilahmad.khan@gmail.com, mukhan@ssuet.edu.pk (Corresponding Author),

shariq@neduet.edu.pk, siva@utem.edu.my

ABSTRACT

Within the neoteric decade, cloud computing has grown as emerging technology which is an on-demand availability of network resources, particularly data storage without any management by users. However, the occurrence of security threats and vulnerability has gradually increased in this processing technology due to its notable growth. In addition to that, the existing Systematic Literature Reviews (SLRs) are only limited with cloud related issues and does not provide their impact on other technologies. This Systematic Literature Review (SLR) examines the security threats experienced by cloud computing along with QoS by edge computing and scheduling. Various consumers and cloud service providers (CSP) obtained benefits from the cloud computing environment. However, various privacy and security challenges occur in this digital age. This SLR mainly aims to review the state of the art research studies on secure cloud computing with high QoS and its challenges. This SLR examined numerous research studies related to cloud computing security with secure service level agreement (SLA) which are published between 2019 to 2022 from the reputed electronic databases. Cloud computing security is ensured mostly based on trust evaluation, implementation of blockchain technology, authentication, and cryptography techniques, and implementing edge computing in the cloud environment. This SLR also analyzed the research gaps of the previous research papers and provides future research directions to obtain secure cloud computing environment with high QoS performance.

Keywords: *Cloud computing, edge computing, blockchain, scheduling, QoS, authentication, service level agreement*

1.0 INTRODUCTION

In recent days, cloud computing is one of the major approaches among various distributed computing methods that work to improve the flexibility and scalability of computer-based on-demand computing by providing standard devices and providing shared resources to the consumers through Internet to minimize the cost. All the services in cloud computing are provided from various data centers which are delivered with the help of cloud service providers (CSP) [1]. Various types of services are provided by the CSP such as infrastructure as a service (IaaS), program as a service (SaaS), platform as a service (PaaS), etc., [2]. Cloud computing consists of storage which is an essential service in the architecture of cloud computing that allows the consumers to share and store the data.

Cloud computing has develop an emerging technology which is broadly employed in both public and private sectors owing to feasibility of its services, which can probably add comfort at various levels. Furthermore, security of accommodated services is vital concern for CSP and cloud users. Security is one of the major problems in cloud computing due to the non-transparent and distributed environment in terms of security, confidentiality, and privacy [3]. Cloud computing services are fundamentally entrenched on internet connection, which are vulnerable to several attacks and threats which reflects on malware injection, data breaches, data losses and etc. Various existing approaches proposed several mechanisms to enhance the security based on access control, data protection, mitigation of attacks, trust delegation, etc., [4].

Cloud data protection is a section of practices that main intention to secure the data in cloud environment. Data protection is ensured by storing the data in the data centers after authorized access [5]. Moreover, the data protection is an integration of policies, procedures and technology solutions that enterprise establishes to secure cloud-based applications and system, with correlated data and user access. In some methods, authentication is performed to increase security [6]. Trust evaluation is performed during processing of data in a decentralized manner. It helps the consumers to choose the secure CSP. In other words, trust is directly proportional to the risk degree. However, there are several challenges are faced by previous works includes integrity, confidentiality, limited control and visibility, encryption, storage and locality which has to considered while ensuring data privacy.

The QoS of the cloud computing environment is affected in terms of various aspects such as security, resource management, scheduling, delay constraints, etc., [7]. For achieving high QoS, a legal agreement must be determined to evaluate the relationship between the consumers and the CSP. In order to meet the above objectives, construction of a service level agreement (SLA) should be established [8]. The QoS of cloud computing environment is further increased by performing efficient scheduling of resources for distributing the resources to complete the tasks (or jobs) with low execution time [9,10]. Several works perform efficiency-aware resource scheduling to increase the cloud computing QoS. However, the delay and overhead constraints remain unsolved in the cloud computing environment.

In order to overcome the aforementioned issues, mobile edge computing (MEC) is introduced in cloud computing environments that have enough storage resources with sufficient communication capability and computing potential [11]. In several works, task offloading is performed to reduce the overhead [12]. In addition, edge computing increases the QoS in terms of low computational power and delay. However, the edge resources are easily attacked by the attacker which reduces the security. In order to increase the security in the edge-cloud environment, blockchain is implemented which provides decentralized storage with high supervision of data [13]. According to existing works, security events in cloud environment has been grown remarkably across the past few years perhaps because of notable growth in the cloud services. In this survey, we have demonstrates the integration of several technology with cloud computing for enhancing the QoS performance of cloud-based application which are lack in existing survey. Besides, we regulated a survey on cloud computing to address several types of security issues, threats and attacks to this developing technology, with potential protection mechanisms and future research direction has illustrated to solve such problems faced by existing works thereby enhancing security in cloud environment.

1.1 Barriers in Cloud Computing

Cloud computing adoption is prevented by various types of barriers and delay constraints [14]. Several barriers preventing cloud computing are described as follows:

(i) *Privacy and Security Issues*

Most organizations considered privacy and security concerns but, several organizations lack of considering the security issues are one of the risk barriers and they did not have any viable solutions.

(ii) *Reliability and Trustworthiness*

Cloud system outages have occurred in several organizations due to publicized documentation and corresponding cloud outages with respect to non-trustworthiness and poor reliability which act as a barrier to implementing the cloud computing approach in large enterprises.

(iii) *Integration and interoperability*

In cloud computing, the public to private or private to public clouds have a high cyber security risk which provides vulnerability in terms of security, poor service provisioning, between APIs and cloud users, cloud users to CSP, etc.

(iv) *SLA, QoS, and Governance*

Security regarding SLA along with poor QoS and governance occurs due to lack of efficient lifecycle control of services in the cloud computing environment. Fig. 1 represents the possible barriers that are presented in adopting cloud computing technology [14].

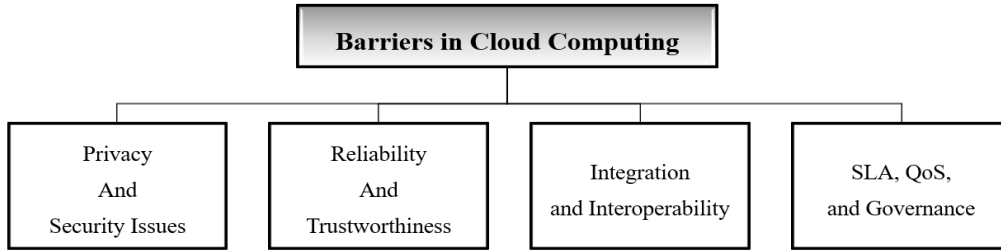


Fig. 1: Barriers in Cloud Computing

2.0 BACKGROUND

The general background knowledge of the main paradigms is mentioned in this section before getting into main sections. For the sake of simplicity, each paradigm is mentioned with diagrammatic representations. The main reason for background section is to guide the ease of the main concepts. The sub-sections are mentioned below:

2.1 Cloud Computing

Infrastructure expansions of many Information Technology (IT) companies are getting higher more and more in recent years. Hence, there will be a robust technology that satisfies the company's needs by minimizing the cost constraints that must be developed [15]. At that time, cloud computing came into picture. The services offered by cloud computing technology are inevitable today which provides both hardware and software services over the internet. Users can utilize the various applications via cloud computing thus reducing the management cost. By the National Institute of Standards and Technology (NIST), cloud computing is defined as the computing resource pools which enable on-demand, and omnipresent computing resources (i.e., servers, applications, networks, and services). Cloud computing consists of four deployment models, four service methods, and five major characteristics which are clearly explained below [16].

(i) *Cloud Characteristics*

The National Institute of Standards and Technology (NIST) defines the five different cloud computing characteristics [17]. The cloud service provider not only provides computing resources but also provides commercial computing technologies. The five main characteristics of cloud are:

- **On-demand Self-Service:** The resources can be provisioned to the demanded users without consulting with cloud service providers. The computing resource may include database, virtual machine, space, containers, etc... The cloud-aided organization can make use of cloud web portal as an interface to know about their resource usage (i.e., services, provision, etc...,) [17].
- **Broad Network Access:** At different communication networks, cloud computing offers services by different platforms of a cloud customer. To be more specific, the cloud services are available in highly broadband links (i.e., internet), and also available in local area networks (i.e., offered by private clouds). The broad network access characteristics of cloud computing enable high QoS to the users as it manages the bandwidth of the network and latency.
- **Resource Pooling:** Cloud computing offers multi-tenancy services in which diverse cloud customers are allowed to share same computing resources and infrastructure without compromising security and privacy. The CSPs' resources can handle multiple services from the customers without affecting their QoS.
- **Rapid Elasticity:** The high scalable nature of cloud computing offers more elasticity to its users. In particular, cloud computing can provide services to the users when they are in demand and cut the services when they are not. The elasticity offers to reduce the cost, capacity, and usage constraints by intelligently scaled-down and up with no extra forfeits. The rapid elasticity of the cloud is defined as just-in-time services.

- **Measured Service:** One of the highlighted characteristics of cloud computing is the measure service which means “pay for capacity you use”. Even, you can be provisioned by the small services and charged according to that. Every service you adopt can be monitored continuously by the CSPs and you will be charged according to that.

(ii) *Cloud Service Methods*

Cloud computing offers services to its users based on four service methods which are mentioned below [17]:

- **Platform as a Service (PaaS):** Based on customer-created applications, the infrastructure is deployed by the CSPs. There is no need to manage the infrastructure such as storage, apps, data, etc., by the users in this service but users can control and place their applications in the PaaS environment. The PaaS offers number of components such as virtual desktop services, databases, web services. However, lack of monitoring the potential on system and applications of cloud workload is the major security concern in PaaS [17].
- **Software as a Service (SaaS):** The infrastructure can be allowed managed by the cloud users in SaaS. Cloud users cannot be allowed to authorize infrastructure and virtual applications. In addition, the user needs to worry about the software and hardware updates and patches. The social network environment, e-mail services, and business network management are coming under SaaS model. Anyhow, there are many issues raised in SaaS due to storing security policies without any privacy measure, the challenges are improper access management, data storage, data and privacy breaches and data retention [17].
- **Infrastructure as a Service (IaaS):** The services, computing resources, backup, storage, and network are provided by the IaaS model. The users are aided with software operations and implementation guidelines. The application deployed, and operating system is only managed by the users while the cloud infrastructure is not allowed to be managed by them. The companies that demand full software support can go with IaaS. In IaaS, data leakage is the vital issue, due to insecure data storage in cloud server and lack of effective control policies on users [17].
- **Container as a Service (CaaS):** This service allows users to manage the containers in terms of edit, upload, stop, and start. The CaaS services are used for creating secure applications through cloud data centers. The processes in the CaaS are empowered through APIs and virtualization tools. Containers can be widely used in DevOps environment of many IT organizations. Even though this platform is significant, the security risks are increased gradually while the containers share same kernels as operating system [17].

(iii) *Cloud deployment Models*

There are four deployment models in the cloud computing environment. All the four models are different from one another as they differ in various features and implications. Based on the user demand and basis, they can select what kind of cloud deployment model would be used [18]. The models are named as below:

- **Public Cloud:** Public clouds or normally clouds was viewed as the superlative deployment model in which the CSPs manage all the services publicly. Education-related information such as blogs, study tolls, and virtual laboratories are coming under public cloud infrastructure.
- **Private Cloud:** The clouds owned or leased by the particular organization are known as private clouds in which the computing tools are not shared with the public. The users in the private cloud have to manage security and infrastructure. Students or organizations who want to create or experience private servers or apps come under private cloud.
- **Hybrid Cloud:** The combination of both private and public clouds is hybrid cloud. The users or organization that owns the hybrid cloud can share insensitive information and hide sensitive information through hybrid clouds. Business platforms that want secure and public communication come under hybrid clouds.
- **Community Cloud:** The community clouds are provided services to the users who are demands with same services. The infrastructure can be varied in terms of off-site and on-site. The community clouds are managed by a group of individuals or organizations. Even though, the cloud deployments models are providing optimal services, day by day the security risk are amplified owing to unauthorized access, misconfiguration, accounts hijacking and external data sharing [18].

2.2 Edge Computing

The issues in the cloud to users in terms of latency are alleviated by adopting edge computing. Recently the growth of edge computing has gone into high demand as a lot of organizations invested in edge computing. The main reason for demanding edge services for its closeness behaviour in which the edge servers are closely placed to the network organization, homes, and public environments whereas the cloud cannot. The popular definition of edge computing is “Technology that serves as the mediator

between user and clouds” by reducing the latency. One of the main reasons for adopting edge computing is, solely most of the user devices are resource-constrained such as smartphones, tracking devices, etc... There are three main edge computing components such as cloud server, local edge server, and devices. Fig. 2 represents the edge-cloud architecture model [19]. The real-time base stations and access points are acts as edge servers that provide latency-free reliable communication to the underlying network devices. Unlike cloud servers, the edge servers also provide delayed intolerant services to the users such as gaming, virtual reality, and augmented reality [19]. However, the edge servers are mostly distributed over a broad geographic area, that making it complicate to secure them. In addition to that, lack of ensuring edge server legitimacy increases the security breaches in the network where the servers can effortlessly compromised and access are gained by the attackers.

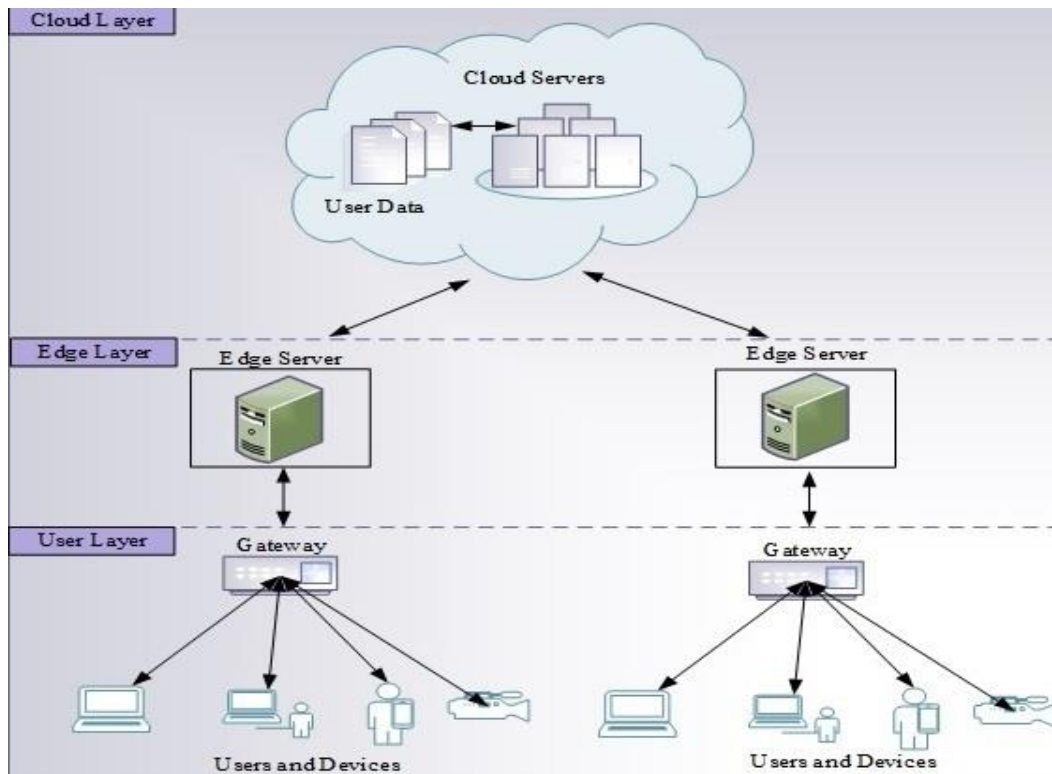


Fig. 2. Edge-Cloud Architecture

2.3 Blockchain

Blockchain is the distribute peer-peer ledger technology used for Bitcoin transactions in the year 2008. The word “Blockchain” refers to the chain of blocks which are interconnected and hashed with cluttered cryptographic algorithms. Nowadays blockchain technology was adopted by many industries and organizations. Especially, the CSPs are given more attention to the blockchain technology due to its trust and transparency nature. Traditionally, blockchain technology was used for managing the digital assets which the blockchain technology was referred to as blockchain 1.0. However, in current digital world blockchain can be used as software programming language which is adopted for many software-related applications called blockchain 2.0 [20].

Some of the features for creating the blockchain-based architecture are:

- **Smart Contracts:** Smart contracts technology was not an inbuilt technology in the blockchain whereas the smart contract technology can be incorporated into the blockchain to train some specific policies. Based on the policies, the smart contracts effectively manage the blocks in terms of security and scalability.
- **Validity of transactions:** Any information stored in the blockchain is in the form of transactions. As numerous protocols are restrained in the blockchain, any new transaction must be confirmed before getting stored as blocks. Thus, the validation capability of blockchain improves the system model.
- **Eternal timestamp:** Once the new transactions are accepted and stored as blocks. The blocks are stored in an orderly fashion chain in which the records are time-stamped and immutable. So, block tracing is difficult in blockchain.

Some of the characteristics of the blockchain which make the blockchain technology unique are given below:

- **Privacy:** The privacy of the blockchain-aided organizations and users is not revealed easily as the blocks are not easily traceable. Every blockchain user was identified by their block-specific address without revealing their user anonymity.
- **Security:** Blockchain technology uses powerful cryptographic tools with which transactions have not tampered easily. The user identity and block address are not directly associated with each other which makes it highly secure technology. Further, if any of the interconnected blocks gets tampered which would not affect the neighbouring connected blocks.
- **Distributed nature:** Blockchain ensures decentralized architecture. There is no central entity for transaction verification which makes the data to be more credible among the blockchain participants. In addition, the consensus mechanism in the blockchain makes the suitable for handling large-scale data with improved management and security measures.
- **Ensure Auditability:** The transparency nature of blockchain technology ensures suitability. The records in the blockchain technology are easily audited by the blockchain experts transparently. The records log maintains all the records including misbehaving a record which improves the auditable nature of blockchain.
- **Consistent rules:** The consistent rules in blockchain technology makes it high persistent and immutable. So, falsification of data is not possible in blockchain. All the hashing functions are represented by the hash unique identifiers, so modification of the data led to difficulty in blockchain.
- **Ensure Auditability:** The transparency nature of blockchain technology ensures suitability. The records in the blockchain technology are easily audited by the blockchain experts transparently. The records log maintains all the records including misbehaving a record which improves the auditable nature of blockchain.
- **Consistent rules:** The consistent rules in blockchain technology makes it high persistent and immutable. So, falsification of data is not possible in blockchain. All the hashing functions are represented by the hash unique identifiers, so modification of the data led to difficulty in blockchain. The blockchain are mainly utilized for secure data storage, however the usage of conventional blockchain results in high block generation time furthermore, its suffer from lack of confidentiality thus affects the scalability which overall degrades the security of cloud data storage. Fig 3 represents the blockchain technology benefits and main features [20].

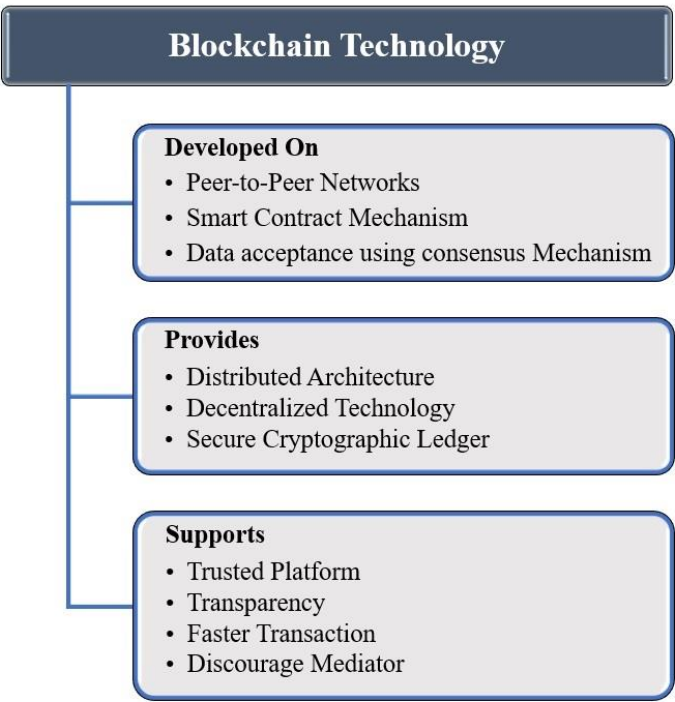


Fig. 3: Key Benefits of Blockchain

3.0 RELATED WORK

Cloud computing is an important need for network resource accessibility including the storage and power used for processing the data. However, it experienced computation complexity with high response time and low transmission capacity. In order to overcome these issues, edge computing is integrated with cloud computing but, it experienced various security challenges which increase the clients' vulnerability and increases the delay in performing computation.

Various security challenges occurred in cloud computing which reduces the data security due to insecure storage and sharing of data, etc. In [21], the author surveyed the privacy and security challenges due to threats and vulnerabilities along with management and cost efficiency in cloud computing. In addition, the threats and their corresponding solutions to overcome the challenges were also reviewed from the previous approaches. However, this review does not deal with QoS due to poor performance in cloud computing (i.e., scheduling, low delay, etc.). Various types of machine learning algorithms are used to enhance the security of the edge-cloud environment. In [22] the authors reviewed the machine learning algorithms which include various types such as reinforcement learning, unsupervised, supervised, and semi-supervised to overcome the security issues faced by cloud considering various types of attacks such as storage-based attacks, network-based attacks, application-based attacks, and VM based attacks. The previous works are compared and provide future directions regarding security. However, this review lack of considering the edge computing security and QoS of the network. Fuzzy logic is applied in cloud computing to resolve various challenges such as security, privacy, reliability, etc. The analyses of fuzzy logic implementation in cloud computing were reviewed in [23] and concluded that the fuzzy logic was applied in most of the existing works to resolve different problems with high-performance optimization. However, this review lack of considering the security issues during data sharing and storing, and it does not include future works based on enhancing the performance of cloud computing.

Trust management in cloud computing reduces the security risks with high data privacy by evaluating trust to ensure storage, security, privacy, and virtualization. In [24], the authors surveyed the trust nomenclature with its dimension and classifications from the previous works and evaluate the trust to compare the existing works regarding cloud environment. In addition, an ML-backed model for verification of trust in cloud computing was proposed based on addressing research gaps to resolve the trust issues. However, the QoS of cloud environment remains insufficient in this review due to lack of efficient scheduling.

Cloud computing security is further increased and ensured by implementing blockchain which provides security in a decentralized manner. The security of cloud computing based on trust management with blockchain was reviewed in [25] by considering various challenges faced by the traditional trust model (i.e., centralized model) such as high management overhead, single point of failure, network congestion, etc., and provide future directions based on edge-based trust management and double blockchain in the cloud computing environment. However, this review lacks QoS consideration. Several security challenges are identified and mitigated in cloud computing to improve the security along with blockchain which was reviewed in [26]. The identified security threats include data leakage, data tampering, data storage, and data intrusions in cloud computing environment. Based on the findings, several future directions are provided based on improving the confidentiality and integrity of data. Table 1 illustrates the systemic study of this literature survey.

Table 1 Systemic study of literature survey

Reference	Date	Topic Area	Article Type	Number of primary studies
[21]	2020	Security challenges in cloud computing	SLR	12
[22]	2021	Opportunities and challenges in blockchain	SLR	7
[23]	2020	Investigation of fuzzy logic in cloud computing	SLR	15
[24]	2021	Trust management in cloud computing	SLR	6
[25]	2021	Blockchain entrenched trust management in cloud computing	SLR	21
[26]	2021	Security risk and mitigation strategies in cloud computing	SLR	5
[27]	2021	Enhancing SLA in SLA for cloud computing	SLR	8
[28]	2022	Job scheduling in cloud computing	SLR	9
[29]	2021	Scheduling in cloud computing	SLR	6
Our work	Security issues in cloud computing with integrated edge computing and blockchain technology		SLR	38

The service level agreement (SLA) was used to ensure the relationship between the consumers and cloud service providers (CSP) to improve the QoS. The review of QoS improvement in SLA by addressing various challenges and research gaps faced in the existing works was performed in [27] to propose a model based on deep reinforcement learning with an enhanced agent with optimal CSPs to increase the performance for achieving high QoS. However, QoS also includes security and efficient scheduling of tasks which are not considered in this survey. In addition, this review does not include any future research directions.

The QoS and performance of cloud computing are enhanced by performing efficient job scheduling. In [28], the authors reviewed the scheduling technique of jobs in cloud computing based on priority rule by evaluating the existing works and finding several problems such as resource wastage, insufficient performance, etc. However, this review lack of consider the security during scheduling of jobs in the cloud computing environment. The scheduling in cloud computing also consists of high efficiency in terms of security awareness, cost, energy consumption, SLA maintenance, etc. Various previous methods performed scheduling based on heuristic, meta-heuristic, and hybrid approaches. Various types of algorithms used in state-of-the-art methods for performing efficient scheduling in cloud computing was reviewed in [29] and compare the strategies based on outcomes. In addition, open challenges and future directions are highlighted by addressing the research gaps. Fig 4 illustrates the taxonomy of the existing survey works.

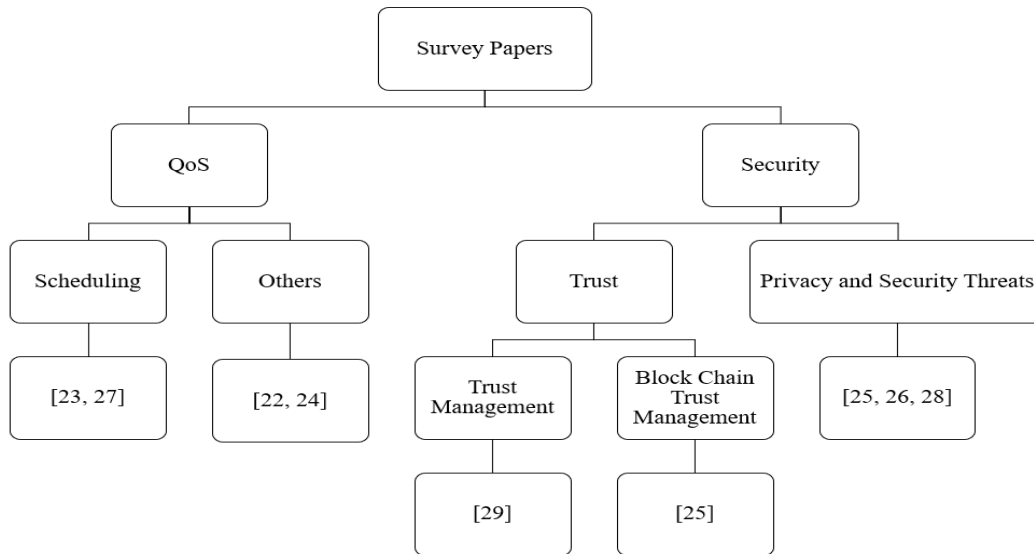


Fig. 4: Taxonomy of Related Surveys

4.0 RESEARCH METHOD

The objective of systematic literature review (SLR) is an explicit, reproducible, and systematic method for evaluating, finding, investigating, and synthesizing the existing works related to cloud computing security and performance. It is an unbiased and fair way for evaluating state-of-the-art methods. We conduct the SLR on cloud computing security with edge computing and their QoS performance based on specific guidelines. This SLR study research method consists of several sub-sections which are described below:

A. Valuable Research Questions

The major objective of this SLR is to validate the security concerns in cloud computing and edge computing based on trust and blockchain along with the QoS performance due to efficient request scheduling. In addition, this research also concerns the strategies applied for ensuring high security from the important existing works. In order to meet the SLR's aim and objectives, three research questions (RQ) are formulated which are described below:

- RQ1- What are the existing cloud computing security threats faced by the existing works and their counter measures?
- RQ2- How the edge computing increases the QoS of the cloud computing environment in terms of all aspects?
- RQ3- How blockchain technology provides security to cloud computing?

B. Search Methods

This sub-section mainly focused on keywords used for searching, electronic reference sources, and process of reference search. The aforementioned processes are described briefly in the sub-sections which are as follows:

(i) Search Keywords

The strings and keywords used for searching are extracted from the generated research questions. In addition, it includes alternatives and synonyms from the research questions. Further, similar keywords are taken from the related literature on security and QoS in cloud and edge computing along with scheduling topics. The keywords used in this SLR are represented as follows:

“Cloud computing security” AND “QoS in cloud environment”, “Cloud computing security” AND/OR “trust-based secure cloud models”, “Cloud computing security” AND “blockchain technology”, “Cloud computing security” AND/OR “scheduling in cloud computing”, “Cloud computing security” AND “edge computing in cloud environment”.

(ii) Reference Electronic Sources

Reference papers search is performed from various popular electronic libraries. There are seven electronic databases such as Scopus, IEEE Xplore, MDPI, Science Direct, Springer, Wiley, and Google Scholars. These digital libraries are the basic source for the published topics related to the domain of computer science.

(iii) Reference Search Process

In order to retrieve suitable literature from various journals, books, and conferences related to this SLR we perform a search process on several digital libraries. Based on this process, we retrieved 150 studies. Further, these studies are filtered for removing the irrelevant references for selecting appropriate papers which are clearly described in the following sections.

C. Study Selection

The study selection is performed in three phases. The first phase is based on the title of the research study, the second phase is based on the abstract of the corresponding research study, and the final phase is based on the full text of the research study. The inclusion and exclusion criteria are derived after the second phase and based on these criteria study selection is performed in which the derived criteria are described as follows. Table 2 denotes the numerical representation of inclusion and exclusion criteria.

Table 2: Numerical Representation of Inclusion and Exclusion Criteria

Database	Papers retrieved	After 1 st phase	After 2 nd phase	After inclusion and exclusion
Scopus	90	80	70	50
IEEE Xplore	60	40	20	13
Science Direct	30	20	16	9
Springer	25	15	15	9
MDPI	15	12	8	3
Google Scholar	10	8	5	3
Wiley	10	7	4	2

(i) Inclusion criteria

The study selection is performed by considering several inclusion criteria for selecting eligible studies which are sorted as follows,

- Studies that discussed cloud computing and its security.
- Studies include blockchain technology in cloud computing.
- Research studies that include edge computing in secure cloud environment.
- Studies discussed the issues and challenges regarding cloud security.
- Studies performed scheduling of requests (i.e., task or job) regarding cloud computing QoS.
- Studies that consider trust to ensure the cloud and SLA security.

(ii) *Exclusion Criteria*

The study selection also considers several exclusion criteria which are excluded to select the appropriate research studies. The exclusion criteria of this SLR are sorted as follows,

- Studies repeated once (i.e., duplicated studies)
- Studies published before 2019.
- Studies using blockchain technology without cloud computing domain.
- Studies without focusing security on cloud computing environment.
- Studies were published in other languages except for English.
- Studies that do not support all three research questions.

(iii) *Quality Assessment Criteria (QAC)*

Based on the results of inclusion and exclusion criteria, we select 68 relevant papers. After selecting 68 studies, we perform QAC to ensure the strength and quality of the selected studies. The checklist of QAC is designed based on the research questions with respect to the corresponding domain area problems. The checklist questions mainly aim to filter the appropriate studies for including them in this SLR. Here, the QAC is applied to select the relevant studies for the evidence in secure cloud computing, edge-cloud environment, and cloud computing QoS. Several questions are proposed with feedback points ranging from 0 to 2 for selecting suitable studies and the scores are determined based on the feedback answers. If the study scores 2 points, then it comes under good quality papers, if it scores 1 point then it comes under normal quality papers, and if the study scores 0 then it comes under poor quality papers. We include the studies in this SLR only if it gets 1 or 2 points. Finally, we include about 48 studies in this SLR after performing QAC in which most of the research studies score 2 points and are collected from IEEE and Science Direct digital libraries. The questions proposed for QAC are sorted as follows,

- Is the research study about cloud computing security approach?
- Does the research study focus on the problem area regarding security in cloud computing?
- Is the research study focus on the QoS of cloud computing environment?
- Does the research study include blockchain technology for secure cloud computing?
- Does the research study include secure scheduling in cloud environment?
- Does the research study include edge computing in cloud environment?

D. *Data Synthesis*

This sub-section aims to combine the shreds of evidence collected from the selected studies for answering the corresponding research questions. In this SLR, data were extracted from the studies in terms of both quantitative and qualitative. Based on various types of strategies, all the extracted data are synthesized. Data about the first and second research questions are synthesized with respect to the narrative method based on cloud computing and its security, edge-cloud environment, QoS, and models for cloud security. Whereas, the data about third research question are synthesized based on secure cloud environment based on blockchain technology.

5.0 RESULTS AND DISCUSSION

This section provides the answers to the research questions in form of results and discussions. The existing works in cloud security, their adopted technologies, and methods used are briefly illustrated in this section.

Research Questions:

A. What are the Existing Cloud Computing Security Threats Faced by the Existing Works and Their Counter-Measures?

The cloud computing technology provides services to the cloud users without any user management which is inevitable and robust to high-scale operation. However, its vulnerability due to security constraints was a major concern. The data leakage in cloud computing could cause severe security threats. Therefore, authentication plays a major role in cloud data security and provides access controls. Hence in [30], biometric authentication scheme was introduced in which the biological information of the user such as iris, palm print, and fingerprints are acquired and undergo several processes. The sender encrypts the data and uploads it to the cloud server, in the same way, the receiver submits their biological information, gets decryption key, and decrypts the sender data. However, the general biometric authentication scheme was easily tampered with by the attackers by impersonating the users. The threats due to data sharing online were severe issues that degrade the QoS and impact user trust. So that, authors in [31] proposed

mutual authentication techniques by adopting machine learning and cryptographic algorithms. The machine learning algorithm detects the security threat during agreement phase using voting ensemble method. Based on the successful key agreement, mutual authentication is initiated by acquiring the security credentials. Once authenticated, the online data sharing was allowed between servers using Elliptical curve cryptography (ECC) and Schorr's signature algorithms.

The selection of appropriate cloud service providers (CSP) ensures the QoS of the cloud users in terms of cost-effective and highly robust services. However, selecting the trusted CSP was still a challenge in cloud environments. Even though, the SLA agreements build relationships among CSPs and cloud users. However, the SLA violation by some of the ambiguous CSPs is also a major concern. The authors in [32], proposed a multi-criteria decision-making approach based on best and worst methods, and TOPSIS was introduced. The reliable and trusted CSP was selected based on their integrity, reliability, trust, and policies. This work ensures the QoS of the cloud users by enhancing the accountability, usability, security and privacy threats, financial, and performance. The trust during the task scheduling needs to be ensured as the scheduling rules and certificates are issued by the third parties. The selection of trusted CSP must be considered some elements such as availability, integrity, and confidentiality. The researchers in [33], compute trust value of the CSP by utilizing genetic algorithms based on their availability of attributes, self-assessment, reputation, and endorsement. Along with a cluttered system, intelligent rules are generated to predict the unknown events to improve the user QoS. Based on the trust value and intelligent rules, users can select the optimal CSPs without any reluctance. Besides, task scheduling for the cloud users also affects the QoS constraints as the task by non-trusted nodes are scheduled.

The resource-intensive tasks of the users are scheduled based on the trust value using fundamental trust management approach in [34]. The trust values of the tasks are computed and the lively scheduler provokes task scheduling for the trusted nodes based on the task constraints such as time, energy, and trust value. The trusted tasks are offloaded securely among the mobile clouds. The researchers in [35], proposed machine learning-based trust evaluation model for e-commerce platforms. Quantitative trust computing alters the qualitative trust computation model by adopting machine learning prediction of behavior methods.

The combination of trust assessment and reputation of CSP-based methods in [36] reduces the security threats by improving the user QoS. The scheduling of big data services in the cloud environment was a vast task as it increases the utilization of resources to peak. The big data platform includes Google cloud and their task in the medical environments are collected and analyzed. Eventually, the trust of the scheduler plays a major part by considering the virtual machine trust value which reduces the QoS of the users. To resolve this issue, the authors in [37], proposed a trust-based big data scheduling scheme based on three levels such as trust of virtual machine, priority of task, and scheduler trust. The metaheuristic algorithm plays an invincible part in optimizing the scheduling in cloud environments. However, the later metaheuristic algorithms for task scheduling optimize the scheduling but lacks with considering security issues. To address this issue, three researchers in [38], adopt a fuzzy-based metaheuristic approach named analogous squirrel search optimization algorithm. The reason for incorporating fuzzy rules is to interact with the network's dynamic nature. The QoS of the cloud users was achieved by considering energy consumption, security issues, imbalance degree, and time of makespan.

The demand-based cloud system was the emerging solution for cloud security. Regarding that, the virtual private clouds provide secure storage and provisioning among the CSPs and cloud users [39]. In that, the tasks by the cloud users are considered jobs and provided to the scheduler. The secure services initiated by the virtual private clouds eliminate the attacks. The integration of machine learning methods and metaheuristic algorithms improves security and decreases the complexity during scheduling process. The adoption of virtual private clouds was one of the key methods to compromising SLA and QoS. Group of researchers in [40], proposed machine learning-based joint methods for cloud computing such as resource allocation, task scheduling, and security constraints. The combined scheduling, resource allocation, and security approaches gained lot of attention from the different cloud vendors as the demand by the stakeholders went high. The stakeholder aimed to reduce the cost by improving the security which was addressed by combining lightweight authentication scheme, metaheuristics algorithm for task scheduling, and deep neural network for resource allocation. The multi-cloud computing had faced lot of security threats as the multiple cloud vendors handle highly resource-intensive tasks. The SLAs in the multi-cloud computing environment are highly violated which reduces the QoS of the cloud users. The issue in multi-cloud environment was addressed in [41] by proposing a multi-round and matching algorithm. The appropriate virtual machines are matched based on the user tasks and security constraints using metaheuristic algorithms.

Cloud computing needs a proactive attack detection mechanism that detects the attacks in advance using intrusion detection system (IDS). The adoption of IDS in the cloud computing environment reduces the security threats. However, the semanticity of the network traffic (i.e., same context information of normal and malicious data) bypasses the IDS. The issue due to semanticity was addressed in [42] by proposing hybrid methods such as long short-term memory, convolutional neural networks, and support vector machine. The accuracy of IDS-based attack detection was a major concern. For that, the authors in [43], adopted an ensemble learning approach. Four classifiers are adopted such as RUS boosted, bagging tree, subspace discriminant, and boosted tree. The final predictions were done by voting-based methods. The high data industrial system requires increased auditing scheme over the

untrusted cloud servers. The product consistency was audited periodically to attain the considerable QoS however, the security issues were a major concern. At to end of this author in [44], proposed novel S-ACICS framework which supports the secure and reliable experience for the cloud auditor. Table 3 represents the existing works in cloud computing security.

Table 3: Existing Cloud Computing Security Frameworks

Reference	Security Measure	Research Purpose	Disadvantages
[31]	Biometric authentication	Cloud data security	• Encryption techniques were very simple and easy to break
[32]	Machine learning-based mutual authentication method	Secure data transmission	• High complexity and easy to impersonate
[33]	MCDM and BWM methods	Trusted CSP selection	• Increased SLA violation
[34]	Genetic algorithm based security	Trusted CSP selection	• Less Convergence and not enough parameters for trusted CSP selection
[35]	Fundamental trust management approach	Secure task scheduling	• Lack of communication security
[36]	Machine learning based trust evaluation	Malicious behavior prediction	• Poor QoS
[37]	Trust evaluation and reputation	CSP selection	• Poor credibility
[38]	Trust-based big data scheduling	Secure task scheduling	• Highly time intensive
[39]	Secure Fuzzy based metaheuristic task scheduling optimization	Secure task scheduling	• Considering inadequate security metrics
[40]	VPC	Secure storage and provisioning	• High cost and easily vulnerable to DoS attacks
[41]	Machine learning-based secure joint resource allocation and scheduling	Secure task scheduling and resource allocation	• Poor QoS and SLA violation
[42]	Multi-round and multi-matching algorithm	Reducing SLA violations in multi-cloud environment	• Poor security measures and QoS
[43]	Hybrid machine learning models	Attack detection using IDS	• Lack of communication path security
[44]	Ensemble machine learning model	IDS	• High complexity
[45]	S-ACICS framework	Secure cloud auditing	• Easily vulnerable to compromise attacks

B. How the edge computing increases the QoS of the cloud computing environment in terms of all aspects?

Secure cloud computing is performed to increase the data security and performance of the application with high quality of service (QoS). However, the QoS of the applications reduces due to various issues regarding complexity, latency, insufficient security, etc. In order to overcome these issues, secure edge computing is introduced in the previous works.

Various cyber-attacks reduce cyber-security in the cloud-edge environment. In [45], the authors performed secure data sharing to increase the cyber security by designing a multi-level trust model which consists of five levels such as fully trusted (FT), FT cloud infrastructure provider (CIP), partially trusted (PT) collaborators (PTC), FTCIP-untrusted collaborators, PT, and non-trusted. The trust level was selected by the data owner with appropriate cyber threat information (CTI) analysis using Homomorphic encryption. In addition, the sanitization approach for the CTI data was performed by either cloud service provider (CSP) or edge device based on the trust level. However, this infrastructure is large and complex and lack of efficient policy templates leads to low security.

The edge-cloud environment is used to process the IoT data in real-time however, it increases the data leakage risk due to the vulnerability of cloud and edge servers. Hence the authors in [46], a secure scheme was introduced to perform secure data search and sharing in the collaborative edge-cloud storage (CECS). This scheme generates a private and public key pair and used the public key encryption (PKE) technique for flexible and secure searching of data. The experimental analysis of this work shows that it has a low computing cost which increases the performance thereby increasing the QoS.

In addition, the security is also reduced due to non-trusted storage between the devices and edge servers and insecure edge computing that increases the security risks during the process of data storage. In order to overcome the above issues, trustworthy architecture of storage in a distributed manner is implemented in [47] with reinforcement learning in the intelligent transportation systems (ITS) along with Hadoop distributed file system (HDFS). This also increases the QoS by storing the data in the secure storage dynamically with the help of reinforcement learning and trustworthiness. In addition, the space allocation of storage, and resource scheduling were also improved by the proposed architecture. Here, the entities of ITS are authenticated by the protocol of identity authentication to attain secure ITS access.

In [48], the security regarding the data which are stored in the cloud is increased by implementing an encryption technique as Edge enabled Searchable lightweight Public-key Encryption (ESPE) in the IIoT environment which was used by the IIoT device to select the nearby edge servers for achieving fast and secure computing. Whereas, the edge computing trust is evaluated in [49] using capsule network based on multi-property technique. The elliptic curved cryptography system was established to ensure the existence of identical trust. The trust property objective expression was established by considering the factors which affect the evaluation property of trust in service applications or resource requests and the capsule network was used to evaluate the correlation between objective trustworthiness prediction and the trust properties.

The security of the edge-cloud environment is ensured by performing authentication of the IoT devices which helps to integrate the IoT with cloud and edge computing technologies in a secure manner. However, the authentication protocol increases the complexity when providing security against attacks that leads to low QoS. In order to overcome the aforementioned issue, lightweight authentication protocol was implemented in [50] that increases the QoS in terms of security, time, and communication cost. Here, the trust center was established in the edge layer which computes the trust value for each device during authentication.

More number of applications used the cloud-edge environment which increases the data in a rapid manner that leads to poor data management due to centralized edge computing. In order to manage the data efficiently, collaborative and decentralized data management was proposed in [51] to improve the overall performance of the mobile healthcare system. In addition, investigation of secure uploading and data sharing was performed using incentive mechanism optimally based on Stackelberg game theory which helps to perform decentralized trading of data.

The architectural models of the IoT, edge, and cloud computing used both on-premise and cloud resources by realizing everything as a service (EAAS) However, it reduces the QoS in terms of cost, security, and performance. In order to overcome these issues, cloud-edge formalization was proposed in [52] for the IIoT environment by deploying the application optimally. The overall cost is reduced by implementing optimization strategy which consists of three various types of objectives based on application owner's particular goals such as reducing the overall cost of the solution, increasing the security score of the solution, and increasing the solution's quality with respect to the multi-criteria based objective function in terms of security and cost to improve the QoS efficiently.

However, the allocation of resources faced various challenges regarding delay and security. In order to reduce the delay with high security, resource allocation was computed based on optimization strategy in the edge-cloud computing of internet of health things (IoHT) devices in [53] with high privacy protection. The requirement based on computation of the IoHT devices were allocated to edge computing and allocate the resources by considering energy consumption, computing, and communication delay. The security of resource allocation is ensured by designing a model based on data privacy including instant messaging regarding the data leakage in IoHT.

In [54], distributed coded edge computing was performed to ensure security and efficiency using matrix multiplication for task computation. Task allocation was performed using an efficient algorithm which was developed based on theoretical analysis and scheme of coded computing was designed using the results of task allocation securely. However, edge-cloud environment experiences some complexity due to heavyweight applications which reduce the QoS. In order to increase the QoS, partitioning of application mechanism is implemented in [55] considering the security aspects based on healthcare applications using dynamic partitioning of application-based secure task scheduling algorithm (DAPWTS) which also consists of mini-cut algorithm for secure data migration during partitioning of application. This algorithm performs energy-efficient scheduling with high-security themes by searching the edge-cloud node and also schedules the failures with low power to reduce the energy consumption thereby improving the QoS.

Mobile devices in the environment compute resources for performing multiple tasks however, it increases the complexity which was reduced by implementing task offloading from mobile devices to the edge nodes with high security in [56] using profit maximization (PM) method. Designing the security model for time overhead measurement for every task and formulate the problem of PM by considering the task deadline constraints and security issues. Finally, secure task execution was performed using PM based genetic algorithm (GA-PM). Table 4 represents the existing works in edge-cloud computing security.

Table 4: Existing Cloud Computing Security Frameworks

Reference	Security Measure	Research Purpose	Disadvantages
[47]	Five-level trust model design	Secure data sharing	Insufficient security due to large and complex infrastructure
[48]	PKE technique	Secure data search and sharing	Low QoS due to high time consumption for key pair generation
[49]	Trustworthiness based on authentication protocol	Secure storage	Poor security due to insufficient credentials for authentication
[50]	ESPE-based secure computing	Storing secure data	Insufficient security due to lack of considering the storage trust
[51]	Trust evaluation with Elliptical curve cryptography (ECC)	Evaluation of edge computing trust	Poor QoS by high latency due to Elliptical curve cryptography (ECC) nature
[52]	Lightweight authentication protocol	Secure edge-cloud computing environment	Poor security due to centralized edge server
[53]	Trusted authorities with Stackelberg game theory-based data trading	Data management with edge server scheduling, secure uploading, and data sharing	Poor scheduling due to insufficient parameters
[54]	Security policies	Resource Allocation	High latency during deployment of optimal objective
[55]	Instant messaging-based data privacy design	Resource allocation	Poor resource utilization
[56]	Coded computing design	Task allocation	Lack of considering priority leads to reduce the QoS
[57]	DAPWTS algorithm for providing security	Application partitioning and secure task scheduling	Poor performance due to low convergence of obtaining optimal results
[58]	Design of security model based on GA-PM algorithm	Task offloading	Low performance due to high time consumption for task offloading

C. How blockchain technology provides security to cloud computing?

Blockchain provides immutable security to cloud computing due to its transparency, integrity, confidentiality, and highly trusted data access. Blockchain technology enhances cloud security by dropping the third-party involvement. Several research works adopt blockchain, cloud computing, and edge computing to reduce the security issue and improve the data management capability. Research work in [57], proposes a blockchain-based task scheduling in which the task scheduler was modeled by adopting blockchain. The offloading was done among the inter could in which blockchain modules are offloaded. The blockchain validates every schedule by introducing proof of schedule consensus.

The SLA violation due to unsecured data storage in cloud environment leads to high-security threats. Recently, the security of Facebook and G-mail users was breached which leads to poor QoS for the Facebook and G-mail users. The research work in [58] addressed the cloud privacy issues by adopting blockchain technology. The secure data outsourcing was done by utilizing hybrid cryptographic algorithm named ECC-AES in which all users are provided with inimitable digital signature. With that digital signature, the outsourcing data are stored in the blockchain as decentralized blocks. The cloud services in terms of data security in the smart city environment posed various challenges in recent years. As the cloud user rate went high, there was a huge traffics faced by the CSPs which leads to data privacy threats in the smart city cloud environment. To cope with the issues in the large-scale environments, the authors in [59] proposed a blockchain-based distributed secure data transmission method in the all the cloud service providers in the smart city environment are connected to the blockchain. The blockchain-connected CSPs validate the client request and provide appropriate services. The secure data request was transmitted to cloud to user and vice versa in encrypted manner.

Managing SLA in the dynamic cloud environment was a critical task as the client service are changing over time. Hence, the users faced some QoS-related issues. Some of the real-time SLA management systems are often faced with single point of failure which leads to SLA violation. Researchers in [60], proposed a dynamic SLA management method based on the dual-stage blockchain method which includes dynamic SLAs change over different periods. In the first stage of dynamic SLA management, the services are provisioned through smart contract-based methods while in second stage, the evaluation of smart contracts was done from an objective function. Similarly, in [61], the SLA violations are addressed by adopting blockchain technology in which fewer scalability and credibility issues are addressed. The adoption of blockchain technology for SLA monitoring improves the fault tolerance and trust rate among CSPs and cloud users. In addition, blockchain technology maintains log data in its database which maintains the violated SLAs and normal SLAs that are utilized in future cloud services for avoiding unwanted computations. Finally, the results are evaluated and provided services to the end-users. The researchers in [62], enable the resilient data auditing method by adopting blockchain technology. The large-scale environments are frequently demanding cloud services for data auditing however, the flexibility and security issues are a major concern. The blockchain-based decentralized data auditing method was an emergent solution that reduces the reliance on third-party auditors thus reducing the security threats. Further, the decentralized nature of blockchain improves scalability as well.

Even though the blockchain technology provides security, resiliency, and data management to the cloud environment, the latency issues faced by blockchain clouds were inevitable. So, cloud-edge computing platforms increase in demand. The combination of those technologies (i.e., blockchain edge-cloud) provides latency-free services to the users thus improving the QoS. The combination of cloud-edge could handle huge volume of data from the IoT. However, the security issues due to handling huge numbers were not so efficient. The issue was addressed in [63], in which physical Unclonable (PUF) is utilized to authenticate the IoT devices and users. Here, blockchain technology was introduced to verify the IoT user and node registrations through smart contracts and provides session keys for secure authentication. The researchers in the work [64] resolve the scalability issues and single-point failure faced by the third-party trusted entity by proposing decentralized blockchain-based authentication in edge-cloud environment. However, the anonymity of the users and service providers are major problem as the malicious attackers tamper with them and gain access to the sensitive data which results in poor QoS and SLA violation issues. The decentralized blockchain technology was utilized in this work in which every entity in the network (i.e., CSPs and edge servers) are uniquely identifiable to blockchain. The respective edge servers gained access only if they are authenticated. Further, the services offered by the CSPs are stored in the blockchain as transactions and also maintain in their database. This could resolve the anonymity and traceability issues. From real-time application point of view, edge-cloud computing and blockchain technology expanded sparsely in vehicular networks. This expansion paves the way for future automation which reduces the issues in road environments. However, due to the large volume of the data, the management and security issues were greatly higher. Researchers in [65], addressed that issue by proposing machine learning, optimization, and authentication techniques. The blockchain technology was used for authentication in two tiers, one-time password was generated using machine learning techniques, and particle swarm optimization algorithm for finding the secure and optimal CSPs.

The data caching and data trading gained less attention due to low latency services by the cloud computing as it limits with high load and cost. The integration of blockchain and edge computing resolves this issue and provides latency-free services in terms of trusted access to data, integrity, and confidentiality [66]. The data cache optimization was done by utilizing Quantum Particle Swarm Algorithm (QPSO) in edge-cloud communications whereas the trust and security issues are addressed by integration of blockchain technology.

The combination of secure storage and sharing method was proposed by researchers in [67]. The resource-constrained nature of IoT devices leads to several security and management problems which were addressed by proposing unique private key method. Every IoT device is given with unique private key which was submitted to edge node. The edge node processes the data and performs Homomorphic encryption. The appropriate service was provided to the users if their key was valid. The encrypted data was securely uploaded to the cloud server. Although there are many techniques and technologies are introduced to improve the security of edge-cloud and blockchain environments are lacks poor data management and privacy issues. To be more specific, the federated learning approaches in the cloud environment compromise privacy and data management issues. The work in [68] incorporates blockchain-based federated learning method in edge-cloud environment. The secure offloading was done between the edge servers and cloud servers in which all information from the edge servers and periodically transmitted to the other edge servers. This kind of transmission reduces the outdoor and indoor security attacks thereby improving the user QoS. Table 5 denotes the blockchain and edge-aided existing cloud computing security frameworks.

Table 5: Blockchain-Edge-Cloud Security Frameworks

Reference	Security Measure	Research Purpose	Disadvantages
[59]	Blockchain-based task scheduler	Task Scheduling	• Requires high time for transaction mining
[60]	Hybrid cryptographic algorithm	Cloud privacy issues	• Limited with high encrypted data size and easily breakable algebraic conditions
[61]	Blockchain-based distributed data transmission	Cloud data security	• High latency issues which affect the user QoS
[62]	Dual-stage blockchain-based SLA management method	SLA management	• Security issues occur when the attacker impersonates
[63]	Blockchain connected CSPs	SLA monitoring	• Fewer scalability issues due to storing in traditional fashion
[64]	Secure decentralized blockchain	Cloud data auditing	• Increased SLA violation
[65]	PUF-based authentication using blockchain	Edge-Cloud security issues	• Limited processing of challenge-response pairs
[66]	Decentralized blockchain-based authentication	Trust issues in edge-cloud environments	• Poor communication path security
[67]	Artificial intelligence-based blockchain authentication	Security issues in vehicular edge cloud environment	• Less convergence and lack of trust metrics
[68]	Optimization and blockchain techniques	Secure data trading in edge-cloud environment	• Lack of security constraints in selecting optimal buyer and seller
[69]	Blockchain and Homomorphic encryption techniques	Secure storage and secure data transmission	• Limited with poor performance as it used Homomorphic encryption
[70]	Federated learning and blockchain	Secure data offloading	• Highly vulnerable to poisoning attacks which affect the QoS

6.0 FUTURE WORK

From the aforementioned sections, this SLR reviews the cloud computing security including edge and blockchain with high QoS based on schedule from all the security-related techniques and its research gaps. Based on the research gaps, this section describes the future research directions to improve the security and QoS in cloud computing environments which are described as follows:

1. In cloud computing environment, security is ensured by implementing cryptographic techniques for storing and securely sharing the data. However, it takes high time consumption which increases the computational utility. In order to increase the security without compromising the efficiency, cryptographic techniques must be developed to increase the security of cloud computing environments with high QoS.
2. Blockchain is used in most works to enhance the security of the cloud computing environment in a decentralized manner. In addition, trust evaluation, and authentication are also performed along with blockchain for achieving high security. However, all the existing state-of-the-art methods do not focus on QoS while providing security. The QoS of cloud computing affects due to high mining time of blockchain. This issue can be overcome by constructing the blockchain-based on any linear structure to reduce the mining time which will increase the QoS without compromising the security. In blockchain the operation mechanism i.e., consensus mechanism also occurs major issue in the applications of blockchain. Such issues remain unsolved in blockchain such as how to identify the issues regarding security due to attacks, forged transactions, etc.
3. In order to increase the QoS scheduling of resources and tasks are performed in several works by implementing various scheduling algorithms to avoid overhead and efficient utilization of resources without any wastage. However, the workload is dynamically changed in the cloud computing environment so, the scheduling of resources must adapt large scalable environment with high flexibility. In addition, during resource scheduling, the SLA lacks security due to various violations so, the violation detection in SLA must perform efficiently during scheduling.
4. Edge computing is implemented with cloud computing to form an edge-cloud environment to enhance the QoS. Some works provide security in the edge-cloud environment regarding data sharing and storage. However, the QoS is affected due to heterogeneity nature of the environment with large scalability which reduces the QoS so, the heterogeneity nature is focused on and implements effective secure workload migration to improve the QoS with high security. In addition to that, the legitimacy of edge servers should also ensure through authentication to prevent from server side injection attacks.

The performance of cloud computing environment is increased due to edge computing however, numerous tasks from the consumers reduce the performance. Implementing numerous micro services based on containerization in the edge-cloud environment increases the performance thereby increasing the QoS of cloud computing. In addition, container security is also focused to ensure the cloud computing security with high QoS.

7.0 CONCLUSION

Cloud services plays a vital role in corporate life in recent days which brings opportunities for accelerating the business organizations based on their ability and resources. In this SLR, we reviewed numerous research papers based on various frameworks, approaches, models, and methods regarding a secure cloud computing topic which also includes the threats and security strategies to increase the security along with trust evaluation, authentication protocol, and implementation of blockchain technology. In addition, edge computing and blockchain combined with cloud computing studies is also reviewed in terms of secure data storage and QoS performance of the cloud environment to improve the QoS and security in cloud computing environment. In addition, edge computing combined with cloud computing studies is also reviewed in terms of QoS performance of the cloud environment to improve the QoS in cloud computing environment. The incorporation of blockchain in cloud computing allow for better data security, improved system interoperability, decentralization and much more. Several survey papers are also reviewed based on secure cloud computing. We addressed various research gaps regarding high-security risks and QoS performance in which security risks are based on data leakage and tampering during data sharing and storage in cloud computing environment. Whereas, the QoS performance is based on high cost, high time consumption, poor resource utilization, poor scheduling, and workload adaptive nature. Trustworthiness of the consumers, SLA security, outsourcing of data, and its corresponding issues are the major challenges that are addressed in this SLR. Based on the research gaps addressed in terms of security and QoS, several future directions are included in this SLR.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

REFERENCES

- [1]. Sun, P., (2020), Security and privacy protection in cloud computing: Discussions and challenges, *Journal of Network and Computer Applications*, vol. 160, pp. 102642
- [2]. Joshi, M., Budhani, S.K., Tewari, N., & Prakash, S. (2021). Analytical Review of Data Security in Cloud Computing. 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 362-366.
- [3]. Madni, S.H.H., Latiff, M.S.A., Coulibaly, Y. et al. (2017). Recent advancements in resource allocation techniques for cloud computing environment: a systematic review. *Cluster Computing* 20, 2489–2533
- [4]. Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, Stephen Linkman (2009) Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, Volume 51, Issue 1, Pages 7-15
- [5]. Wang, T., Zhang, G., Bhuiyan, M. Z. A., Liu, A., Jia, W., Xie, M., (2020), A novel trust mechanism based on Fog Computing in Sensor–Cloud System, *Future Generation Computer Systems*, vol. 109. pp. 573-582
- [6]. Mo, W., Wang, T., Zhang, S., & Zhang, J. (2020). An active and verifiable trust evaluation approach for edge computing. *Journal of Cloud Computing*, 9, 1-19.
- [7]. Qi, S., Lu, Y., Wei, W., & Chen, X. (2021). Efficient Data Access Control With Fine-Grained Data Protection in Cloud-Assisted IIoT. *IEEE Internet of Things Journal*, 8, 2886-2899.
- [8]. Veerabathiran, V.K., Mani, D., Kuppusamy, S., Subramaniam, B., Velayutham, P., Sengan, S., & Krishnamoorthy, S. (2020). Improving secured ID-based authentication for cloud computing through novel hybrid fuzzy-based homomorphic proxy re-encryption. *Soft Computing*, 1-16.
- [9]. Mahipal, S., & Sharmila, V.C. (2021). Virtual Machine Security Problems and Countermeasures for Improving Quality of Service in Cloud Computing. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), 1319-1324.
- [10]. Liu, X., Xia, C., Wang, T., Zhong, L., & Li, X. (2020). A behavior-aware SLA-based framework for guaranteeing the security conformance of cloud service. *Frontiers of Computer Science*, 14.
- [11]. Yang, J., Jiang, B., Lv, Z., & Choo, K. (2020). A task scheduling algorithm considering game theory designed for energy management in cloud computing. *Future Gener. Comput. Syst.*, 105, 985-992.
- [12]. Nanjappan, M., & Albert, P. (2022). Hybrid-based novel approach for resource scheduling using MCFCM and PSO in cloud computing environment. *Concurrency and Computation: Practice and Experience*, 34.

- [13]. Sha, K., Yang, T.A., Wei, W., & Davari, S. (2020). A survey of edge computing-based designs for IoT security. *Digital Communications and Networks*, 6, 195-202.
- [14]. Wu, H., Wolter, K., Jiao, P., Deng, Y., Zhao, Y., & Xu, M. (2021). EEDTO: An Energy-Efficient Dynamic Task Offloading Algorithm for Blockchain-Enabled IoT-Edge-Cloud Orchestrated Computing. *IEEE Internet of Things Journal*, 8, 2163-2176.
- [15]. Zhang, P., Pang, X., Kumar, N., Aujla, G.S., & Cao, H. (2020). A Reliable Data-transmission Mechanism using Blockchain in Edge Computing Scenarios. *ArXiv*, abs/2202.03428.
- [16]. Alghamdi, B., Potter, L.E., & Drew, S. (2020). Validation of Architectural Requirements for Tackling Cloud Computing Barriers: Cloud Provider Perspective. *CENTERIS/ProjMAN/HCist*.
- [17]. Golightly, L., Chang, V., Xu, Q., Gao, X., & Liu, B.S. (2022). Adoption of cloud computing as innovation in the organization. *International Journal of Engineering Business Management*.
- [18]. Murthy, C.V., Shri, M.L., Kadry, S.N., & Lim, S. (2020). Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, 8, 205190-205205.
- [19]. Li, C., Bai, J., Chen, Y., & Luo, Y. (2020). Resource and replica management strategy for optimizing financial cost and user experience in edge cloud computing system. *Inf. Sci.*, 516, 33-55.
- [20]. Garg, R. (2022). MCDM-Based Parametric Selection of Cloud Deployment Models for an Academic Organization. *IEEE Transactions on Cloud Computing*, 10, 863-871.
- [21]. Ometov, A., Molua, O.L., Komarov, M.M., & Nurmi, J. (2022). A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors (Basel, Switzerland)*, 22.
- [22]. (2021). A Systematic Review on Blockchain in Education: Opportunities and Challenges. *Nepalese Journal of Management Science and Research*.
- [23]. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, 1-40.
- [24]. Butt, U.A., Mehmood, M.A., Shah, S.B., Amin, R., Shaukat, M., Raza, S.M., Suh, D.Y., & Piran, M.J. (2020). A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics*, 9, 1379.
- [25]. Tariq, M.I., Tayyaba, S., Mian, N.A., Sarfraz, M.S., Hussain, A., Imran, M., Pricop, E., Cangea, O., & Paraschiv, N. (2020). An analysis of the application of fuzzy logic in cloud computing. *J. Intell. Fuzzy Syst.*, 38, 5933-5947.
- [26]. Saleem, M., Warsi, M.R., Islam, S., Anjum, A., & Siddiqui, N. (2021). Trust Management in the World of Cloud Computing. Past Trends and Some New Directions. *Scalable Computing: Practice and Experience*.
- [27]. Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, 10, 1-34.
- [28]. Alouffi, B., Hasnain, M., Alharbi, A.S., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, 9, 57792-57807.
- [29]. Edinat, A., Al-Sayyed, R.M., & Hudaib, A. (2021). A Survey on Improving QoS in Service Level Agreement for Cloud Computing Environment. *International Journal of Interactive Mobile Technologies (iJIM)*.
- [30]. Murad, S.A., Muzahid, A.J., Azmi, Z.R., Hoque, M.M., & Kowsher, M. (2022). A review on job scheduling technique in cloud computing and priority rule based intelligent framework. *Journal of King Saud University - Computer and Information Sciences*.
- [31]. Sana, M.U., & Li, Z. (2021). Efficiency aware scheduling techniques in cloud computing: a descriptive literature review. *PeerJ Computer Science*, 7.
- [32]. Joseph, T.S., Kalaiselvan, S.A., Aswathy, S.U., Radhakrishnan, R., & Shamna, A.R. (2021). A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. *Journal of Ambient Intelligence and Humanized Computing*, 1-9.
- [33]. Singh, A.K., & Saxena, D. (2021). A Cryptography and Machine Learning Based Authentication for Secure Data-Sharing in Federated Cloud Services Environment. *Journal of Applied Security Research*, 1-24.
- [34]. Youssef, A.E. (2020). An Integrated MCDM Approach for Cloud Service Selection Based on TOPSIS and BWM. *IEEE Access*, 8, 71851-71865.
- [35]. JaithunbiA., K., Sabena, S., & Ramesh, L.S. (2021). Trust Evaluation of Public Cloud Service Providers Using Genetic Algorithm with Intelligent Rules. *Wirel. Pers. Commun.*, 121, 3281-3295.
- [36]. Ali, A., Iqbal, M.M., Jamil, H., Akbar, H., Muthanna, A., Ammi, M., & Althobaiti, M.M. (2022). Multilevel Central Trust Management Approach for Task Scheduling on IoT-Based Mobile Cloud Computing. *Sensors (Basel, Switzerland)*, 22.
- [37]. Zhang, F., & Yang, Y. (2021). Trust model simulation of cross border e-commerce based on machine learning and Bayesian network. *Journal of Ambient Intelligence and Humanized Computing*, 1-11.
- [38]. Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach. *IEEE Access*, 7, 9368-9383.
- [39]. Rjoub, G., Bentahar, J., & Wahab, O.A. (2020). BigTrustScheduling: Trust-aware big data task scheduling approach in cloud computing environments. *Future Gener. Comput. Syst.*, 110, 1079-1097.

- [40]. Zade, B.M., Mansouri, N., & Javidi, M.M. (2021). SAEA: A security-aware and energy-aware task scheduling strategy by Parallel Squirrel Search Algorithm in cloud environment. *Expert Syst. Appl.*, 176, 114915.
- [41]. Rajasoundaran, S., Prabu, A.J., Routray, S., Kumar, S.V., Malla, P.P., Maloji, S., Mukherjee, A., & Ghosh, U. (2021). Machine learning based deep job exploration and secure transactions in virtual private cloud systems. *Comput. Secur.*, 109, 102379.
- [42]. Bal, P.K., Mohapatra, S.K., Das, T.K., Srinivasan, K., & Hu, Y. (2022). A Joint Resource Allocation, Security with Efficient Task Scheduling in Cloud Computing Using Hybrid Machine Learning Techniques. *Sensors (Basel, Switzerland)*, 22.
- [43]. Zhu, Q., Tang, H., Huang, J., & Hou, Y. (2021). Task Scheduling for Multi-Cloud Computing Subject to Security and Reliability Constraints. *IEEE/CAA Journal of Automatica Sinica*, 8, 848-865.
- [44]. Prabhakaran, V., & Kulandasamy, A. (2021). Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. *Neural Comput. Appl.*, 33, 14459-14479.
- [45]. Singh, P.P., & Ranga, V. (2021). Attack and intrusion detection in cloud computing using an ensemble learning approach. *International Journal of Information Technology*, 1-7.
- [46]. Cheng, J., Qi, S., Wang, W., Yang, Y., & Qi, Y. (2020). Fast Consistency Auditing for Massive Industrial Data in Untrusted Cloud Services. *Proceedings of the 2020 on Great Lakes Symposium on VLSI*.
- [47]. Chadwick, D.W., Fan, W., Costantino, G., Lemos, R.D., Cerbo, F.D., Herwono, I., Manea, M., Mori, P., Sajjad, A., & Wang, X. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Gener. Comput. Syst.*, 102, 710-722.
- [48]. Tao, Y., Xu, P., & Jin, H. (2020). Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage. *IEEE Access*, 8, 15963-15972.
- [49]. Qiao, F., Wu, J., Li, J., Bashir, A.K., Mumtaz, S., & Tariq, U. (2021). Trustworthy Edge Storage Orchestration in Intelligent Transportation Systems Using Reinforcement Learning. *IEEE Transactions on Intelligent Transportation Systems*, 22, 4443-4456.
- [50]. Wang, W., Xu, P., Liu, D., Yang, L.T., & Yan, Z. (2020). Lightweight Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices. *IEEE Transactions on Industrial Informatics*, 16, 4221-4230.
- [51]. Jia, C., Lin, K., & Deng, J. (2020). A Multi-property Method to Evaluate Trust of Edge Computing Based on Data Driven Capsule Network. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 616-621.
- [52]. Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M., & Kumari, S. (2022). Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment. *IEEE Consumer Electronics Magazine*, 11, 57-63.
- [53]. Li, X., Huang, X., Li, C., Yu, R., & Shu, L. (2019). EdgeCare: Leveraging Edge Computing for Collaborative Data Management in Mobile Healthcare Systems. *IEEE Access*, 7, 22011-22025.
- [54]. Casola, V., De Benedictis, A., Di Martino, S., Mazzocca, N., & Starace, L.L. (2021). Security-Aware Deployment Optimization of Cloud-Edge Systems in Industrial IoT. *IEEE Internet of Things Journal*, 8, 12724-12733.
- [55]. Wang, J., & Wang, L. (2021). A Computing Resource Allocation Optimization Strategy for Massive Internet of Health Things Devices Considering Privacy Protection in Cloud Edge Computing Environment. *J. Grid Comput.*, 19, 17.
- [56]. Wang, J., Cao, C., Wang, J., Lu, K., Jukan, A., & Zhao, W. (2021). Optimal Task Allocation and Coding Design for Secure Edge Computing with Heterogeneous Edge Devices. *IEEE Transactions on Cloud Computing*, 1-1.
- [57]. Lakhan, A., Li, J., Groenli, T.M., Sodhro, A.H., Zardari, N.A., Imran, A.S., Thinnukool, O., & Khuwuthyakorn, P. (2021). Dynamic Application Partitioning and Task-Scheduling Secure Schemes for Biosensor Healthcare Workload in Mobile Edge Cloud. *Electronics*.
- [58]. Li, Z., Chang, V.I., Hu, H., Yu, D., Ge, J., & Huang, B. (2021). Profit maximization for security-aware task offloading in edge-cloud environment. *J. Parallel Distributed Comput.*, 157, 43-55.
- [59]. Wilczyński, A., & Kolodziej, J. (2020). Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology. *Simul. Model. Pract. Theory*, 99.
- [60]. Darwish, M., Yafi, E., Al Ghamdi, M.A., & Almasri, A. (2020). Decentralizing Privacy Implementation at Cloud Storage Using Blockchain-Based Hybrid Algorithm. *Arabian Journal for Science and Engineering*, 45, 3369-3378.
- [61]. Cha, J., Singh, S.K., Kim, T.W., & Park, J.H. (2021). Blockchain-empowered cloud architecture based on secret sharing for smart city. *J. Inf. Secur. Appl.*, 57, 102686.
- [62]. Uriarte, R.B., Zhou, H., Kritikos, K., Shi, Z., Zhao, Z., & Nicola, R.D. (2021). Distributed service-level agreement management with smart contracts and blockchain. *Concurrency and Computation: Practice and Experience*, 33.
- [63]. Khan, K.M., Arshad, J., Iqbal, W., Abdullah, S., & Zaib, H. (2022). Blockchain-enabled real-time SLA monitoring for cloud-hosted services. *Cluster Computing*, 25, 537-559.

- [64]. Kefeng, F., Fei, L., Haiyang, Y., & Zhen, Y. (2021). A Blockchain-Based Flexible Data Auditing Scheme for the Cloud Service. Chinese Journal of Electronics.
- [65]. Zhang, Y., Li, B., Liu, B., Hu, Y., & Zheng, H. (2021). A Privacy-Aware PUFs-Based Multiserver Authentication Protocol in Cloud-Edge IoT Systems Using Blockchain. IEEE Internet of Things Journal, 8, 13958-13974.
- [66]. Bonnah, E., & Ju, S. (2020). DecChain: A decentralized security approach in Edge Computing based on Blockchain. Future Gener. Comput. Syst., 113, 363-379.
- [67]. Li, C., Liang, S.T., Zhang, J., Wang, Q., & Luo, Y. (2022). Blockchain-based Data Trading in Edge-cloud Computing Environment. Inf. Process. Manag., 59, 102786.
- [68]. Gawas, D.A., Patil, H.Y., & Govekar, S.S. (2021). An integrative approach for secure data sharing in vehicular edge computing using Blockchain. Peer-to-Peer Netw. Appl., 14, 2840-2857.
- [69]. Zhang, L., Peng, M., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing. Transactions on Emerging Telecommunications Technologies, 32.
- [70]. Qu, G., Cui, N., Wu, H., Li, R., & Ding, Y.M. (2022). ChainFL: A Simulation Platform for Joint Federated Learning and Blockchain in Edge/Cloud Computing Environments. IEEE Transactions on Industrial Informatics, 18, 3572-3581.

BIOGRAPHY

MUZAMMIL AHMAD KHAN  (muzammilahmad.khan@gmail.com) received the bachelor's and master's degrees in Computer Engineering from the Sir Syed University of Engineering and Technology, Pakistan, in 2000 and 2003, respectively. He is a PhD scholar in NED University of Engineering and Technology, Pakistan. He is currently serving as an Assistant Professor in Computer Engineering Department in Sir Syed University of Engineering and Technology. His research interests include cloud computing, IoT, network security, e-commerce, entrepreneurship and project management.

SHARIQ MAHMOOD KHAN  (shariq@neduet.edu.pk) received the bachelor's and master's degrees in computer science from the NED University of Engineering and Technology, Pakistan, in 2005 and 2007, respectively, and the Ph.D. degree from Brunel University London, U.K., in 2015. He is currently serving as an Associate Professor of computer science for NED University. He has authored or co-authored multiple research articles in international journals and conferences. He is a regular reviewer for a number of international journals and conferences. His research interests include routing protocols design in mobile and vehicular ad-hoc networks, network security, and wireless sensor networks.

SIVA KUMAR SUBRAMANIAM  (siva@utem.edu.my) received the bachelor's of Electronic Engineering (Industrial Electronic) with Honours (B.Eng) from Kolej Universiti Teknikal Kebangsaan Malaysia, Malaysia in 2006. He received Masters of Sciences in Electronics (M.Sc) from Universiti Teknikal Malaysia Melaka, Malaysia in 2009. He received Doctor of Philosophy (PhD) degree from Brunel University London, United Kingdom in 2017. He is currently serving as Senior Lecturer in Faculty of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka, Malaysia. His research interests include IoT, network security and wireless sensor networks.