IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 17, 2021, accepted April 9, 2021, date of publication April 14, 2021, date of current version April 21, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3073203

A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies

BADER ALOUFFI[1], MUHAMMAD HASNAIN[2], ABDULLAH ALHARBI[3], WAEL ALOSAIMI[3], HASHEM ALYAMI[1], AND MUHAMMAD AYAZ[2]

[1]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[2]School of Information Technology, Monash University Malaysia, Subang Jaya 47500, Malaysia
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia

Corresponding author: Muhammad Hasnain (muhammad.malik1@monash.edu)

ABSTRACT Cloud computing has become a widely exploited research area in academia and industry. Cloud computing benefits both cloud services providers (CSPs) and consumers. The security challenges associated with cloud computing have been widely studied in the literature. This systematic literature review (SLR) is aimed to review the existing research studies on cloud computing security, threats, and challenges. This SLR examined the research studies published between 2010 and 2020 within the popular digital libraries. We selected 80 papers after a meticulous screening of published works to answer the proposed research questions. The outcomes of this SLR reported seven major security threats to cloud computing services. The results showed that data tampering and leakage were among the highly discussed topics in the chosen literature. Other identified security risks were associated with the data intrusion and data storage in the cloud computing environment. This SLR's results also indicated that consumers' data outsourcing remains a challenge for both CSPs and cloud users. Our survey paper identified the blockchain as a partnering technology to alleviate security concerns. The SLR findings reveal some suggestions to be carried out in future works to bring data confidentiality, data integrity, and availability.

INDEX TERMS Auditing, cloud computing, cloud models, decryption, encryption, malicious behavior, intrusion, secured communication.

I. INTRODUCTION

Cloud Computing concept has emerged from the distributed software architecture. Cloud computed technology is aimed to provide hosted services over the internet. In recent years, cloud computing in Information Technology has given rise to various new user communities and markets [1]. Cloud computing services are provided from data centers located in different parts of the world. Microsoft SharePoint and Google applications are general examples of cloud computing services.

Security plays an important role in the wider acceptance of cloud computing services [2]. Existing literature is focused on different security solutions, including technology and security policy implementation. The latter study introduced new attacks on the cloud environment from criminological perspectives. The proposed solution to these recent attacks is based on criminal theories for the protection of the cloud. A study [3] identified several security issues affecting cloud computing attributes. The same research proposes to overcome the identified problems concerning the security of cloud. A security guide, developed in this research, enables the cloud user organizations to be aware of security vulnerabilities and approaches to invade them.

Security vulnerabilities and challenges arise from the usage of cloud computing services. Currently, cloud computing models are the primary source of these challenges and vulnerabilities. The intruders exploit the weakness of cloud models in accessing the users' private data, by attacking the processing power of computer systems. The ''Autonomous Cloud Intrusion Response System'' (ACIRS) has been recently proposed to overcome the problem mentioned earlier [4]. Before this work, the ''Network Intrusion Detection and Countermeasure Selection system'' (NICE) [5] worked on the selection of the best countermeasures to mitigate the risks to cloud virtual networks. As compared

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

to NICE, ACRIS is superior in mitigating the risks and challenges to networks.

There is a widespread use of cloud computing (CC) in information technology. However, many service owners are still reluctant to fully adopt the CC as relevant security technologies are not as yet matured. Thus, literature shows a need for service providers to invest in CC-associated device security [6]. We have found a few studies that show the proposal of evaluation of cloud computing security. One of these research studies introduces an ''attack tree map'' (ATM) to analyze security vulnerabilities and threats. Research [7] highlights various facets of CC combined with the trusted computing platform to provide security services such as confidentiality, authentication, and integrity.

II. BACKGROUND INFORMATION ON CLOUD MODELS AND RELATED WORKS

This section presents a short overview of the cloud computing models. We also offer a summary of related works to our research topic.

A. CLOUD MODELS

1) SOFTWARE AS A SERVICE (SaaS)

The SaaS model facilitates users to access the software and other programs in a cloud. Using the SaaS solution eliminates the need for in-house applications, data storage, and support for the application administration. Companies pay to use the SaaS resources on a user basis [8].

2) PLATFORM AS A SERVICE (PaaS)

PaaS is a cloud computing service that supports a full software life cycle and allows users to develop cloud applications and services [9]. Programmers and developers do not need to purchase their equipment; instead, they use intermediary equipment and deliver the developed applications to clients over the internet. In PaaS, an individual or a company is not required to buy the software and hardware to develop the applications. Google App Engine, Azure services platform of Google, Amazon's relational database services (RDS) are the key examples of PaaS model.

3) INFRASTRUCTURE AS A SERVICE (Iaas)

IaaS is the cloud computing service delivered in the form of platform in a virtual environment [10]. Clients are not required to purchase servers, data centers, network equipment or space (e.g. Amazon EC2).

4) CONTAINER AS A SERVICE (CaaS)

Based on container virtualization, CaaS has emerged as a cloud model to resolve application development issues in the PaaS environment. The CaaS cloud model is aimed to free the application by making them independent of PaaS environment specifications [11]. Amazon EC2 Container Service (ECS) and Google container engine are examples of CaaS model.

Studies [8] and [10]–[11] emphasized general cloud security models such as SaaS, PaaS, IaaS, and CaaS. Empirical studies show that these models play an important role in cloud security from the perspectives of cloud security providers and clients. However, a successive range of cloud security models is more important to safeguard the users' activities on clouds. If a security model is more secure, a user will be happier to use the client computing services.

B. RELATED WORK

Information technology has rapid changes in recent years. Cloud computing has added more promising role of IT with the addition of storage for users. Cloud computing has enabled the vendors to rent out their services at hourly rates. They also rent out the space to users on their physical systems. However, these services have several security threats for users. In a report, Cloud Security Alliance revealed that abuse, insecure interfaces, and nefarious usage were the vulnerable threats. These threats have been associated with the application program interfaces and cloud computing [12].

Information security splits into three main objectives, such as integrity, confidentiality, and availability. Security threats to these security goals include a long-term confidentiality issue because one considers that present and past encryption schema are not secure. Information leakage vulnerability is another concern as data is outsourced. Tampering with data also poses threats to data confidentiality [13].

As new technologies are emerging to meet the users' demands, there is a significant increase in cloud security threats. These threats are occurring in the form of several unseen exploitation through the cloud computing services and their associated interfaces. It has become essential to counteract the occurred and potential attacks [14]. Presence of the insecure interfaces is a big challenge to both cloud users and cloud service providers.

Cloud services' security and availability mainly depend on APIs that involve in data access and data encryption on clouds. Further research can be undertaken to ensure the security of these APIs and network interfaces. New security proposals can meet the protection challenges of services from intentional and accidental attacks and violation of terms of services. Furthermore, layered APIs have more complexity as third body operators use cloud services. Actual proprietors cannot access the services. In addition to it, malicious insiders are common threats to cloud services as they violate the services' terms and access the information they are not permitted. Usually, an employee is the malicious insider who steels the confidential information that belongs to a company or its legal users, An inside malicious user can corrupt the information, particularly in a peer to peer file sharing systems [15].

Multi-Tenancy is referred as resource sharing and associated risks of data confidentiality and integrity. Multi-Tenancy has been called a serious concerning issue for professionals in cloud computing. Professionals' understanding about attack surfaces and attack vectors is most important [16]. In [17],

an increased number of cloud computing service users resulted in data security and privacy threats.

Cloud users face issues of reliability from big players in cloud computing. In [18], researchers reported that Amazon's EC2 and S3 suffered an outage for 3 hours and 8 hours in February 2008 and July 2008, respectively. Google's Gmail services remained unavailable for 3 hours, which prevented 113 million users from accessing documents through their Gmail accounts. Microsoft and Amazon offered their customers access to selecting the geo-spatial location of companies' data centers.

1) CLOUD SERVICE USER

Cloud service users, either clients or attackers, must have users' authentication privileges to access the cloud services. Communication between users and cloud resources seeks the secured channel that keeps the users' login information more secure than hypertext transfer protocol (HTTP) users. Secondly, communication between cloud services and users must be ensured with synchronization [19].

C. INTRUSION DETECTION SYSTEM

Cloud service manager as a cloud provider must follow the service level agreements (SLAs) and conform to technical standards. Cloud data on cloud premises needs to be protected from physical and crypto-graphical intrusion attacks [20]. Resource starvation or crashing the server may prevent the legal client from accessing the cloud computing services. Cloud services would have an intrusion detection system that identifies users' vulnerabilities and sends an alert message to cloud service admin to take swift action against the attackers or intruders. Cloud service manager rejects the access of such intruders if they are found to be real intruders. An authenticated user is given access to desired data files. Data encryption approach for both client and server ends is chosen. To detect intruders' anomaly behavior through encrypted traffic, an intrusion detection system discovers attacks by analyzing a large number of data patterns. In [21], information extraction from encrypted data traffic is obtained through features of HTTP traffic and frequency of access. In the following, we discuss how an intrusion detection component is designed and implemented for encrypted traffic. An intrusion detection system is classified into three tiers as given in the following.

1) DATA AT REST

The intrusion detection system scans the data from cloud data storage sources, encrypts the data, and removes it encrypted when it is found non-trusted. However, fine-tuning and configuration constraints are real concerns for data at rest.

2) DATA IN MOTION

Clients' real concern lies in data security in moving data from client to cloud or cloud to client. Network monitoring of sensitive information via emails, and instant messaging, a system requires the identification and prevention of log email information that attempts to leak information from a client or an organization by the aid of steganography.

3) DATA IN USE

Data transmission from the client-side computer is monitored via the output peripherals such as USB ports, printers, CDs, and external storage devices. If the applications access sensitive data, it is filtered before sending it to relevant peripherals [22]. A plain-text message transmits information between a portable device and EC3 unit, and data leakage can occur when a legal cloud computing services user stores the data at remote-based storage devices. However, data leakage is prevented by using the algorithms developed in [23] to identify the legal cloud storage devices. Cloud database maintains the list of legal devices and requires the authentication of portable devices before data exchanges between clouds and cloud clients. After verification of devices, the cloud client retrieves and transmits the data. When a cloud client wants to upload data, the EC3 unit sends a request to connect a cloud manager. Cloud client passes a plain text denoted by the Pm to EC3, where a chip of encryption/decryption encrypts the Pm to a random positive integer k.

Fig. 1 shows us the device authentication process with several steps. The first step focuses on extracting the device information, followed by the ID decryption in the second step. The final step involves the decryption in the ECC integration unit. Under these seven steps, for the authentication process, a legal user cannot read, copy, or transmit personal records to a system because data-writing is disabled on the storage. Therefore, a legal user even needs the primitive root g from p and prime number p before accessing the system's records. A private key of an integer value that ranges between 2 and p – 2 is used to publicize the (g, p, B). A seven step process involves an authentication process of devices, as shown in Fig. 1. A new user is asked to fill the form for account creation. Credentials of a new user are stored in the cloud system [24]. The choice of elliptic curve cryptography with (2m) fields is compatible with the modern computers and logic gates of binary states [25].

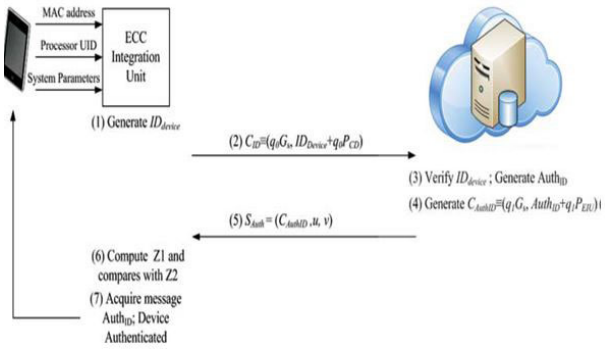

FIGURE 1. Authentication process for devices.

4) AUDITING AND UNIT TESTING

Cloud providers should have control over the auditing and maintenance of cloud services. It can be achieved through the

consecutive monitoring of users' logs and administrative sessions with those parts of cloud services affected by users. The trace-back technique is applied to identify users who violate the policies and laws. Cloud testing is a hope to determine the balance of advantages and risks of cloud computing services. Cloud service providers and customers perform cloud testing at their levels.

On the other hand, the customer is responsible for performing tests to avoid or mitigate any risk to its organization or customers. In a cloud security model, the cloud services provider ensures the architecture's physical security through auditing procedures and controls to overcome the cold-boot attacks. The cloud service manager is responsible for setting the default baseline of security measures for users. Cloud service managers monitor tenants' malicious attacks when they target different services to flood the other tenants' virtual machines [26]. In [27], researchers proposed that the protection of multi-tenancy areas was the major focus of cloud vendors.

Cloud services are well-known approaches for product traceability of industrial systems to provide data integration and sharing services [28]. However, malicious cloud services prevent industrial participants from the correct acquisition of traceability of products. Recent research proposes Acics as consistent and fast auditing schema for the massive industrial information in the untrusted cloud computing environment. This schema enables the industrial participants to play an auditor role for consistency checking of products. Experimental results show that the proposed Acics compared to other approaches is efficient in data consistency checking of small amounts of products at a reasonable cost. The proposed Acics schema shows better read or write latency rate. This schema has been not tested on large products, and hence it can be examined in the future works.

Before the latter reviewed study, research [29] highlighted that cloud computing has an alarming security risk to customers' data. Customers transfer their data to CSP's provided storage but remain unaware of evaluating the CSP's security controls to protect their sensitive data. The cloud security alliance (CSA) sets the guideline to gauge the CSP's organization's security controls. It enables a cloud service user to trust the services of CSPs. The main issue is that CSA's questionnaire-based security assessment is not validated for the responses' accuracy. A framework proposed in the same study aims to bridge this gap by using third party auditors (TPAs) for validating the participants' responses. Still, there is no way of using the outcomes of third party checking for external users. To make users more trusting in an organization's cloud services, we need to get their feedback for further quality evaluation of cloud providers' services.

5) CLOUD RESOURCES MANAGEMENT

Cloud computing services models concern the management of cloud resources. Cloud service providers offer clients resources such as virtual machines, network devices, load balancers, and firewalls. Resource management is one of the pressing issues of IaaS [30]. Services availability directly links to the security of physical equipment and devices at premises of cloud service providers. Denial of service attack makes resources unavailable for the intended consumers of cloud computing services. Attackers get access to protected resources by exploiting system leakage, bugs, configuration mistakes, and design flaws [31]. In [26], the denial of service attack issue is subject to tenant machines and compromised virtual machines. An inside or outside attacker floods the virtual machine with the attacked traffic of TCP, UDP, and ''internet control message protocol synchronized'' (ICMP SYN) floods. The attacker also chooses to allocate more resources to virtual machines to generate more attacked traffic. To cope with denial of service from UDP and ICMP traffic, a client or tenant uses the maximum threshold (λ) for ICMP and UDP traffic.

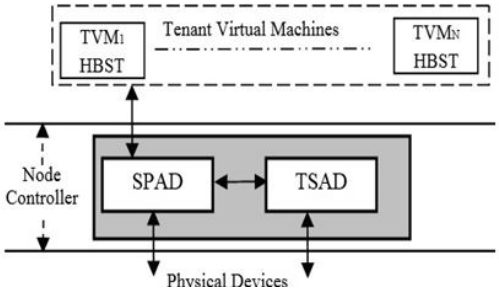

FIGURE 2. Cloud security architecture [26].

Fig. 2 shows us the security architecture proposed in [26]. As shown in Fig. 3, tenants may keep their own host-based security tools (HBST) to run on their virtual machines. They obtain virtual machines from cloud providers. Thus, monitoring a system through the HBST has good visibility. The other essential components of the architecture are service provider attach detection (SPAD) and tenant-specific attack detection (TSAD) [26].

6) SECURITY ANALYSIS

ECC's encryption process efficiently encrypts the different messages by using the varying points of the elliptic curve. A short key size of 256 bits prevents the attacks of algorithms on the ECC encryption system because the computing complexity of attacking algorithms is O (2128). Hence, cloud clients' IDs and private keys are stored in their smart cards. Therefore, an illegal user cannot generate a valid digital signature [32].

The client can also ask the client service provider to drop data if UDP or ICMP exceeds the threshold and produces an alarm by the client administrator. The TCP SYN flooding attacks the tenant and exploits the weaknesses presented in a three-way handshake process. In this case, an attacker floods the victim's machine and overflows the victims through the half-open connections.

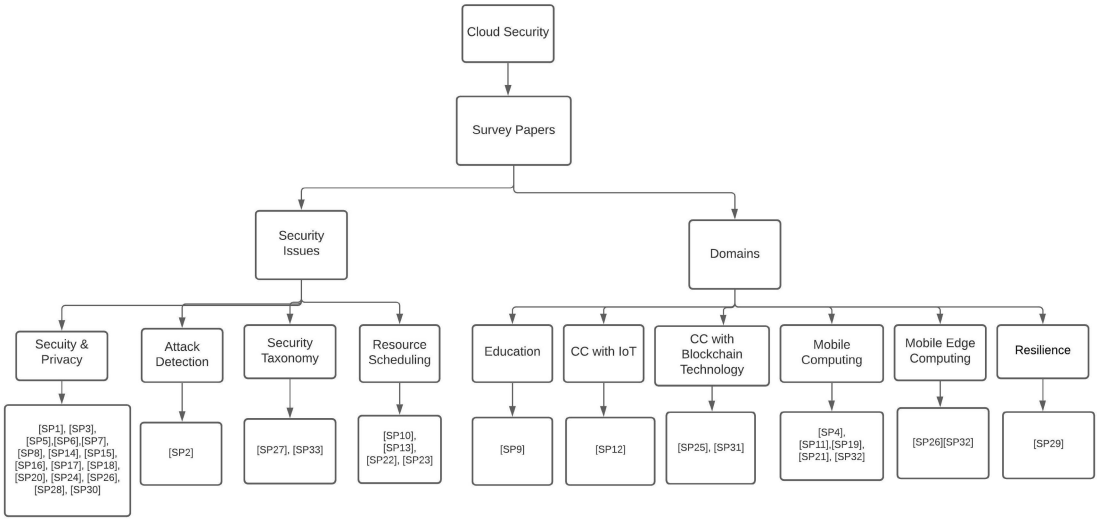

FIGURE 3. Taxonomy of survey literature on cloud computing topics.

7) INTRUSION DETECTION FEATURES FOR ENCRYPTED TRAFFIC

SlowDos attacks are challenging to researchers and they need to be detected using the signature-based approaches for a HTTP encrypted traffic. Recent work [33] introduces artificial intelligence (AI) based approach to cope with the challenge mentioned earlier. The proposed work analyses, processes, and aggregates the data packets to detect the anomalies dynamically. Both clustering and deep learning techniques combine to increase the accuracy efficiency of proposed approach. The proposed approach's evaluation is performed on a real testbed to show the performance and accuracy in detecting the attacks over the encrypted traffic.

8) TAXONOMY OF SURVEY LITERATURE ON CLOUD COMPUTING

Current survey literature bespeaks most of the security and privacy concerns and their mitigation strategies (see Table 5). As observed in this survey paper, a large body of literature is focused on mitigating the security threats on clouds. However, the survey paper observes that the current literature is classified into security issues and other cloud computing domains. Based on multiple security perspectives, the security issues are classified according to the cloud aspects. The majority of authors of the existing survey papers have paid attention to security and privacy challenges. Other than security and privacy issues, resource scheduling is the widely examined area of cloud computing. However, security taxonomy and attack detection are less explored areas, as shown in Fig. 3. It indicated that inadequately classified security challenges could prevail than much spending on security issues.

Moreover, we present the classification of the cloud computing (CC) combined with other research domains. These domains include education, IoT, Blockchain technology, mobile computing, and resilience. Among these domains, mobile computing is a widely studied research area. However, two survey papers [SP25] and [SP31] have been published recently on blockchain technology with cloud computing topics. The former survey paper is a short conference paper that does not show a detailed discussion on blockchain technology's role in overcoming cloud computing security issues. The latter survey paper is a combined effort of researchers on fog computing and blockchain technology. Since several papers have been published on blockchain technology with cloud computing, we present a brief posture of blockchain technology's role in cloud computing.

III. RESEARCH METHOD

A systematic literature review (SLR) as a research study method is used to evaluate and interpret the research topic's available literature. A systematic literature analysis is an alternative to an SLR. Kitchenham guidelines are more specific to conduct this SLR [34]. The SLR protocol for this study consists of the following subsections.

A. RESEARCH QUESTIONS

The main objective of this research is to examine the security concerns regarding cloud computing services. This research also focuses on risk mitigation strategies from significant existing research studies. To cover the aims and objectives of this SLR, we formulated four research questions as follows:

1) RQ1: What are the cloud computing security threats and their mitigation strategies?
2) RQ2: What are the security problems that have not been addressed by commercial cloud providers?
3) RQ3: What are consumers' concerns from cloud computing standards and policies implementation?
4) RQ4 What is the role of blockchain technology in the security of cloud data?

B. SEARCH STRATEGY

This phase is focused on search keywords, electric sources, reference management tool, and a search process. We describe each process in the following subsections.

1) SEARCH KEYWORDS

The search keywords and strings have been derived from designed research questions. We have also included synonyms and alternatives. We took synonym keywords from the relevant literature on cloud computing security topics. We show the search keywords in the following.

''Cloud security challenges'', ''cloud security models'', ''commercial cloud provides and security challenges'', ''cloud security mitigation strategies'', ''cloud security models'', ''blockchain technology''.

2) ELECTRONIC SOURCES

Popular digital libraries have been used to search for papers—these digital libraries are IEEE Xplore, Springer, ACM, Google Scholars, and Science Direct. These digital libraries are the primary source of publications on topics from computer science domain.

3) REFERENCE MANAGEMENT

Using search keywords and their alternative, we found a large number of studies from the above-mentioned electronic sources. We used Endnote X9 [35] as a reference management tool to collate and manage the retrieved material. It enabled us to easily add and remove the studies whenever we required them.

4) SEARCH PROCESS

We launched a search process on the digital libraries to retrieve the relevant literature from journals, conferences, and books. This search process resulted in more than 1500 studies. We used Endnote to manage the pdf files and their respective references, making it easier to read papers. Next, we applied the selection process to filter out the irrelevant papers.

C. STUDIES INCLUSION AND EXCLUSION CRITERIA

We followed the studies' inclusion and exclusion criteria as listed in Table 1.

D. QUALITY ASSESSMENT CRITERIA (QAC)

The QAC criteria is formulated to ensure the quality and strength of primary studies. A checklist has been used in [36] to assess the quality of research studies. The QAC checklist is designed that depends upon the questions related to problems of the domain area. As given in Table 2, these questions aim to sort out the relevant studies to include them in the systematic literature review (SLR).

The quality assessment criteria are applied to determine the essential studies for evidence in cloud computing security concerns and cloud security models. Studies' analysis is based on the proposed questions, and if a study answers Yes, then 2 points are awarded to that study. If the answer is No, then 0 points are awarded and if the answer is partially then 1 point is allocated to that study. Initially, we gathered 1500 research studies, and next, we applied QAC criteria to sort out studies that were suited to answer the research questions. By application of QAC, 71 studies were found to be answering the research questions. Hence, we retained (5%) of total studies suitable for this systematic literature review.

TABLE 1. Studies' inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
Research studies that discuss cloud computing	Studies that are published in other than the English language
Research studies that discuss cloud security issues	Papers with unidentified references
Research studies that examine the incidents of data intrusion in the larger organizations	Articles focusing on other than security topics of cloud computing
Research studies that include cloud security concerns' mitigation strategies	Duplicated research papers
Research studies that include cloud security models	Papers published before 2010
Studies on blockchain technology with cloud computing services	Studies on blockchain technology with other than cloud computing topics

TABLE 2. Quality assessment criteria.

ID	Quality Assessment Criteria	Feedback Score
Q1	Does the study focus upon the domain's problem area?	Yes = 2, No = 0 and Partially = 1
Q2	Is a study explicitly focusing on cloud security issues?	Yes = 2, No = 0 and Partially = 1
Q3	Is the study about Cloud security models or approach?	Yes = 2, No = 0 and Partially = 1
Q4	Does the study involve the cloud security mitigation strategy?	es = 2, No = 0 and Partially = 1

E. DATA SYNTHESIS

Data synthesis is aimed to aggregate the evidence from chosen studies to answer the research questions. The proof is a single piece that provides little evidence compared to the aggregation of many parts of evidence [36]. Data extracted in this SLR is qualitative (weaknesses and strengths of cloud security models or approaches) and quantitative (estimation and accuracy values of cloud security issues). Extracted data have been synthesized by using different strategies. Data about research questions 1-2 have been synthesized through a narrative method. Data is tabulated so that each study is consistent with cloud security domain, cloud security approach and focused area of cloud security models. Visualization tools such as bars and pie charts are also employed to present cloud security issues and mitigation strategies or approaches in the enhanced manners. Data of research questions 3-4 highlight the important cloud security models and its focused issues in each security model. Bar as a visualization tool is employed that shows how many studies have focused on certain cloud security issues.

IV. RESULTS AND DISCUSSION

This section presents our SLR's results and their discussion is given in the following subsections.

Table 3 shows us the studies publication year, security approaches and purpose of the research. In table 3, it has become clear that cloud computing and its security concerns have remained the focus of researchers in the last few years. Second, the chosen studies research focus shows that cloud computing has advantages for both cloud service providers and users. However, cloud consumers' concerns about information security have made them rethink before they use cloud computing services.

A. SECURITY THREATS AND RISK MITIGATION STRATEGIES (RQ1)

Data loss due to its leakage is a severe threat to cloud security. Data compromise and modifications occur without keeping the backup copy by altering or deleting the original information. Also, data storage on cloud media has less reliability because insiders and third parties can access the data. In irresponsible media, the companies' offering of cloud service are regarded as fraudulent [37]. Utility based approach can be used to overcome the latter-mentioned challenge by detecting the malicious behavior of users. This utility allows users to recover their data. Unity service is a personal repository service, which is different from other cloud services.

Cloud services users do not need to become unauthorized users of services, but internal individuals of CSP organization present malicious behavior. In studies [20] and [37], we have found such incidents, which can harm the data security from cloud service providers. Therefore, trust-building between client and cloud service providers is emphasized through a unity model.

The emerging paradigm of cloud computing ensures the reliability, availability, and scalability while users access the cloud computing services over the internet. The concept of software and services is activated on the users' demands. However, several additional risks have been perceived by the productive organization. A hacker can perform tricks to snatch the confidential information as each and every thing is kept inside the cloud computing box. Due to evolution in the security disciplines, hackers can be prevented to have an illegal access to cloud data. Also, more security measures can be proposed to provide a comprehensive security to users regarding their data.The key-splitting and Homo-morphic encryption can be extended to have new breakthroughs in this area of research [38]. In [39], the emphasis was on secure data transfer between customers and cloud computing providers over the secured communication channels.

A group of researchers proposed an attack model in [40], where they identified the three most suspicious customers. Researchers used the datasets from Google and sensed the questionable behavior of customers. Businesses and

TABLE 3. Publications and their research focus.

References	publication Year	Information security approach	Purpose of research
[8]	2013	SaaS, PaaS and IaaS	Cloud services security
[10]	2012	SaaS, PaaS and IaaS	Cloud services security
[12]	2010	Report on cloud security	Security concerns
[13]	2010	Review of security measures	Data Tampering and Leakage
[14]	2011	Emergence of new technologies	Data security threats
[15]	2011	APIs security	Intrusion and actual proprietors
[16]	2014	Multi-Tenancy security	Risk elimination strategy
[17]	2013	Hybrid multi-cloud security model	Date storage security
[18]	2012	Cloud computing culture	Amazon's and Microsoft's clouds security
[19]	2012	Secure Protocols for communication	Data synchronization
[20]	2012	Cloud security architecture	Third party control
[21]	2007	Anomaly detection	Analysis of encrypted traffic
[22]	2014	ECC Approach	Data leakage Prevention
[23]	2013	Security Encryption	Algorithm Information Hiding
[24]	2014	Diffie Hellman and ECC	Secure data exchange in clouds
[25]	2013	ECC Approach	Secure Platform for secure applications
[25]	2014	Security Architecture	Security for cloud providers and tenants
[26]	2014	Security Architecture	Security services
[27]	2010	Review on information security	Governance, risk and compliance issues
[30]	2014	Resource Management	IaaS concerning issues
[31]	2013	A Review approach	Vehicular Clouds
[37]	2012	Unity Mode	Durability and data availability
[38]	2012	key-splitting and holomorphic encryption	Hacking concerns
[39]	2013	Standard Protocol	Client and Service Provider Communication
[40]	2012	Attack model	Identification of suspicious customers
[41]	2012	System review approach	Cloud Computing technology
[42]	2013	Data encryption	Security of remote users
[43]	2014	MapReduce framework based approach	Cyber security issues
[44]	2011	A literature survey	Design decisions of approaches
[45]	2013	UDP and TCP protocols	Secure data communication
[46]	2013	ECC	In Practice

individuals get nervous using the cloud systems, as a cloud is a metaphor in the internet's perspective. They fear any unauthorized users can access the information as cloud computing simply lingers in cyberspace. Respective cloud computing providers ensure security and privacy in cloud computing [41]. If the infrastructure of cloud computing is insecure, the information's availability and confidentiality become at risk. Firewall configuration, server patching, and placement of the intrusion-detection system are enforced. The use of encryption and authentication processes can ensure data availability and confidentiality, as shown in Fig. 4.

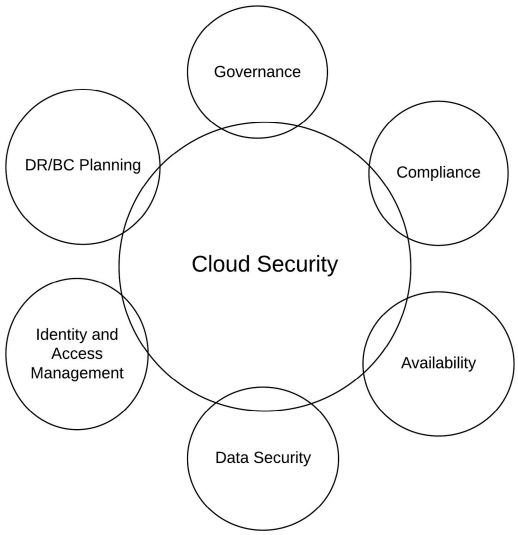

FIGURE 4. Safety in cloud computing.

A remote office requests for cloud computing services from vendors to enable the data encryption sent by clients. The encrypted data is stored at the cloud center. Clients or remote users of cloud computing services get access to the encrypted data [42].

Most significantly, cloud computing in financial organizations is exposed to risk from hackers. Therefore, we have a security approach of encryption and authentication to reduce the risk of alteration or information disclosure in transit and storage. The encryption process provides data security from prying eyes. Entities trying to retrieve the companies' protocol for accessing the information get the scrambled information. This approach accomplishes the use of keys in two ways. Cloud service providers never retain the keys, instead their clients retain keys locally and ensure that used keys are destroyed or rotated correctly. Microsoft and Amazon have made advancements in making the simple storage service (S3) available for customers through REST and SOAP [18].

Maintenance and distinctiveness are critical issues in the implementation of the cryptographic scheme. Replication is a standard in cloud computing for keys' encryption/decryption maintenance. Amazon faced a similar matter, and since then, such a problem has been resolved. However, the lack of foresight in the process of cryptography results in disastrous outcomes [43].

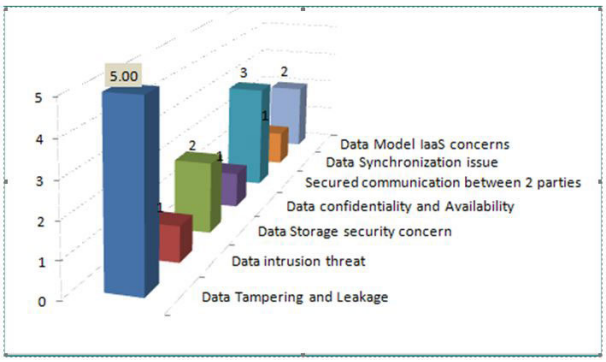

FIGURE 5. Identified cloud computing security threats.

Fig. 5 shows us the seven identified types of cloud computing security concerns in research studies. Data tampering and leakage are the deepest valued concerns for both clients and cloud computing service providers. These types of cloud computing security issues encompass cloud computing users who cannot access cloud computing resources. They are either attackers, hackers, or users who attempt to access the cloud computing services for which they are not registered. Although data intrusion threat has a close resemblance with the earlier types of data tampering and leakage, intruders use different means of entering the data clouds. In [41], data confidentiality and availability have been called primary security concerns irrespective of other security lapses between clients and cloud computing services. A secure communication between clients and cloud computing service providers is the second-highest score regarding cloud computing security risks. We have pointed out the IaaS level concerns as a separate type of cloud computing security risks.

Data tampering and leakage is the real concern of users in several domains. A cloud-based healthcare system may have challenges of patients' data leakage [47]. Forensic data collection and edge computing environments have severe security risks, including forensic data removal or log leakage. The edge cloud services have their local isolation from the cloud, and security monitoring becomes inappropriate. Malicious users target geographically divided management [48]. Besides this, log data cannot be stored securely, and forensic information can be removed from the cloud to prevent forensic investigation.

The second identified threat is the data intrusion in cloud computing. While adopting cloud computing services, an intrusion detection system (IDS) provides a solution to security threats [49]. Various IDS have been developed to recognize accurate attacks. A hybrid approach of intrusion detection is proposed in [50], which suits high traffic data like clouds. Compared with the prevailing techniques, the hybrid approach efficiently detects anomalies and provides better security to increase traffic in a cloud environment. Besides these developments, a suspicious IDS itself can have adverse effects for detection in the cloud. SaaS providing companies include Google, Adobe, Microsoft, Shopify, and HubSpot that still suffer security, loss of control, and connectivity

requirement issues. Researchers can undertake future research to address the security issues arising from cloud computing models, i.e., IaaS.

Data storage, data confidentiality, and data availability in cloud services are among the other identified threats to cloud computing security. For example, outsourcing stored data at the cloud requires an additional security layer to strengthen the data confidentiality. Research [51] introduced a ''cloud storage based on ID-based encryption'' (CS-IBE) with the one file access policy and a user's identity proposed to be used as an encryption key. Although this approach simplifies the key management issues, it shows limited performance for data confidentiality.

A recently published work [52] introduces a new cloud service, namely ''database as a service'' (DBaaS), where a service provider has responsibility to grant access of software, hardware, and network to users. It would enable them to access and manage a database. At the same time, a distrustful service provider keeps the control of database queries. As a result, security issues emerge in the confidentiality of stored data during outsourcing of data to a user.

B. COMMERCIAL CLOUD COMPUTING PROVIDERS AND SECURITY CHALLENGES (RQ2)

A survey study [53] finds that the top five cloud providers, including Amazon, Azure, Adobe, Google cloud platform, and VMWare, are efficient in their cloud services' data security feature. Reliability and performance are among other features. To measure the cloud providers' trustworthiness is still an issue for researchers, and a customer cannot judge it without appropriate tools. Container launched by VMs is an emerging practice offering security sandboxing. Containers enable the cloud providers to continue managing their applications on clouds [54]. Since application management at the edge is challenging for cloud providers, it is done either ad hoc or with the platform. When multi-tenant run their applications on the same host resource, security, and privacy issues arise from their applications. Existing literature on commercial service providers (CSPs) reveals that cloud service models are involved in hampering security concerns [55]. Therefore, it is users' workload based on the sensitive data that they do not need to outsource to a public cloud directly. Outsourcing the consumers' data and addressing the associated risks is challenging for both users and cloud service providers. These risks include shadow-IT, security, control and transparency, and business continuity [56]. Interoperability is another challenge because many consumers are locked to a single CSP due to interoperability issues.

Amazon AWS ''Identity and Access Management'' (IAM) [57] operate the access control mechanism and identity management system. Each customer gets a tenant account upon the subscription of the Amazon AWS product. To assure the security of users' data, they are allocated security credentials to access AWS resources. However, Amazon IAM is not so expressive and contains simple featured-based policies with the limited encryption attributes. AWS and Microsoft Azure policies clearly state that customers need to address the security of their data, operating system, application, and their configuration, identity, and access management in a shared responsibility. The AWS only considers the hardware, software, and networking facilities security [58]. Cloud users mistakenly assume that their public IaaS providers have responsibility for securing their data, operating system, and applications [59]. ''Secure by design'' [58] is an innovative idea that needs to be integrated with all cloud services and applications to enable an agile environment for businesses in the face of security threats and the technology ecosystem. Thus, researchers can undertake future research to develop security architecture to ensure built-in security from developing systems and services, tools, and technologies across the cloud environment. Before the latter mentioned studies, a research article [60] focused on software security requirements and proposed replacement of traditional software development with the emerging services. Thus, cloud providers can share a security service with the distributed stakeholders.

C. CONSUMERS' CONCERNS FROM CLOUD COMPUTING STANDARDS AND THEIR POLICIES IMPLEMENTATION (RQ3)

Standards and policies are the significant measures for users and admin of CSPs. These policies and standards also apply to partners with CSPs. In a cloud model, policies are configured to monitor end-users devices and cloud computing services [32]. Service level agreements are one of the obstacles that contain the scope of cloud services. Cloud services' consumers come across while adopting cloud computing services. Data unavailability, vendor lock-in and insufficient measures of security create concerns for users. Consumers show their concern over the lack of interoperability and standards. Portability features are provided with limited offers. Therefore, evaluation of SLAs benefits the service providers in terms of legal actions, while minimal assurance of data protection for consumers is specified to reflect the consumers' requirements at the right time [13].

National laws also conflict with the SLAs that enforce the cloud computing service providers to disclose their customers' sensitive information [61]. Cloud computing processes and elements like APIs did not follow the cloud computing standards that presented a barrier for clients to switch cloud suppliers without expense and pain [9]. Although most vendors have defined their standard mechanisms, they could not complete the function of writing standards once and run it everywhere [41]. Data security, privacy, and up-time were typically called the essential items in [44]. In addition to these advantages, cloud client did not require the initial capital to invest in the infrastructure. Cloud clients shift their risks to cloud computing service providers.

Literature reveals that cloud computing and social media have become an influencing factor in controlling and monitoring public policies. Social media applications are widely used and have become a significant source of data generation.

Cloud computing can store the generated data that can map useful public opinion in different aspects such as issues and their solutions, advantages and disadvantages, and proposals. Research in [62] proposed to combine CC services with social media, and monitor the public policies efficiently. For the evaluation of the presented approach Tweets data is used. Thus, data from other platforms such as Facebook and Instagram have been not used. Although CC has several advantages for users, it still suffers from unreliable latency, network communication cost, and mobility support.

Extrinsic concerns such as network, compliance, and information security arise while implementing the CC services in small, medium enterprises (SMEs). Security and cloud services professionals and SME representatives should consider these issues before implementing cloud services [63]. Decision making in an organization is mainly based on information security. On the other hand, cloud users have no experience of handling their data on cloud storage. It leads to an ambiguity in the minds of users. Thus, the cloud provider must ensure users' information by installing data safety measures.

Although CC has many deployment and implementation benefits, organizations adopting them face compliance, trust, hosting, legal, security, and privacy issues [64]. Policymakers also state about the inadequate resources and guidelines to inform decision-makers. A comprehensive framework is proposed to investigate the CC services, their deployment, and delivery models. The proposed framework has been adopted by the Saudi Government agencies overseas. Among issues faced by the adopting organization, data security and privacy has been considered the leading factor when deciding whether to adopt it. Legal and policies are other issues that may not allow the adoption of CC services due to security and privacy concerns during the implementation.

D. ROLE OF BLOCKCHAIN TECHNOLOGY IN THE SECURITY OF CLOUD DATA (RQ4)

Security is one of the major challenges of big industries, including banking, supply chain management (SCM), electronic health records, and smart applications in recent years. A research [65] proposes a novel framework to monitor the activities taking place at the particular data evidence. This data evidence comes from data and users' signature based on the SHA-256 Cryptographic Hash Algorithm. A cloud-based ''software defined network'' (SDN) is created with the support of a Blockchain controller, cloud server, and an authentication server (AS). Researchers propose to register all users with the AS to obtain the secret key. In this proposed framework, the ''Elliptic Curve Integrated Encryption Scheme'' (ECIES) technique encrypts data packets and transfers them to a cloud server. The experimental result showed that better performance concerning throughput, response time, accuracy, and total change security features has been achieved. Security features in the blockchain-based cloud include authentication, network security, access mechanism, and privacy method. This work is comprehensive and can be implemented for a real-time application with the improved security. Traceability of users due to modification in data has become possible, increasing the reliability and preserving the users' data privacy. However, a SDN controller that may suffer from various DoS and DDoS attacks can be prevented by extending it in future works. However, we carefully require to handle the computational overheads and avoid the increasing cost.

Resource allocation and task scheduling are challenging issues to academia and industry. Security during the task scheduling on a distributed computing environment has been considered a significant criterion for personalizing cloud services. Blockchain technology integration with the cloud clusters helps secure the cloud transactions and access the application and data codes [66]. Recent work proposes a novel blockchain scheduler that is better in performance compared with other cloud scheduling models. One of the limitations of the proposed research is its simulation, which could be near a realistic one but cannot be 100 percent applicable to real-world case studies. Therefore, researchers can consider realistic scenarios with different cloud clusters and cloud technologies to develop a multi-cloud system in future works.

Given the increased number of published works, we cannot capture all relevant research papers. The possible reason is that Blockchain technology is booming nowadays among scholars and industrial professionals. We have selected a few recently published works to show the integration of blockchain technology with the cloud computing environment. However, cloud computing is a separate research area and much work is in progress on the latter mentioned area. The majority of research studies [65]–[69] have been focused on securing the cloud data through the blockchain technology. The effective use of blockchain technology provides an extra security layer to data at clouds, and users' trust remains intact while outsourcing the information. A legitimate user achieves the relevant information.

Data sharing systems such as electronic medical records (EMRs) facilitate users to access the medical record and store the patients' information effectively [72]. Moreover, data exchanges occur between connected mobile devices in the cloud computing environment. Still, blockchain security and privacy concerns remain to be settled in future research works. It is essential to protect the users' identity. A study [73] proposed an attribute-based approach to secure the users' identity. The proposed approach, based on the KUNodes, has an attribute master key and an attribute signing key. These attributes' revocation can be easily achieved by using the KUNodes algorithm. The proposed approach is security preserving, unforgeable, and collision resistant.

Cloud-centric computing has several downfalls. One of them is the issues produced from the unilateral test. This is because an application is delegated to a user in the cloud environment. Cloud-centric computing is not scalable when a single point failure occurs [74]. To overcome these issues, decentralized computing is utilized in different Internet of Things (IoT) scenarios. Devices connected can be

locally managed instead of using third-body services, thereby resulting in conveniently available applications and services.

Blockchain technology is optimizing the resource allocation to customers. Auction algorithms ensure the appropriate allocation to the actual buyers of computing resources. A study [75] introduced the broker concept in managing and adjusting the trading market. Besides, the proposed research introduces edge-cloud computing and blockchain technology to address the issues of real-time processing and allocation of resources. The proposed research designed a trading market where buyers compete with the sellers' resources. An iterative auction schema works to collect the buyers' requirements and then allocate the resources accordingly.

Trust and security are real issues to the IoT Big Data. Trust concerns have been addressed by proposing the permissioned blockchain to perform data invoking and data storage and avoid data tampering from inner-side users and external attackers [76]. Even if data is tampered with on some partial nodes, the entire ledger still works and provides security and trust to users because tampering can't reach and succeed at all. However, the proposed approach still has security issues while releasing the key for encrypting data at the user layer.

Blockchain technology provides the necessary privacy and security to the communication between fog nodes, IoT devices, and cloud computing. The research carried out in [77] is not entirely successful as it is still in progress. The proposed framework in the latter study has not been implemented in a real-world environment. This is due to the big head size issue of blockchain structure. This problem has not been resolved yet.

Latency demand is another crucial issue for blockchain technology stakeholders. Different scenarios are used to evaluate the proposed blockchain architecture [78], and smart contracts. Minimized latency is needed when communication and computational capabilities are transferred close to the sensor nodes. To ease the network scalability, mobility, and location awareness, minimized latency is required for the devices connected in a physical environment. Therefore, low latency is favorable to cloud computing users.

A security layer is added by blockchain technology to the data transactions on distributed cloud storage. A trusted third party is no more required as a smart contract is employed that ensures the reliability and fairness of data trade. The proposed research in [79] reduces the cost of transferring the data on cloud storage. However, blockchain technology suffers the limitations in communicating the same data contents as claimed by the buyers. An attacker can resell the data privately using other venues.

We have summarized and presented the proposed approaches on data security issues regarding cloud computing. Since the last few years, cloud computing with big data has grown dramatically, and data security remains a paramount concern. Cloud services availability has conflicting constraints for the varied services. A semantic-based access control (SBAC) approach [80] acquires the financial services in clouds. The proposed approach enables the access

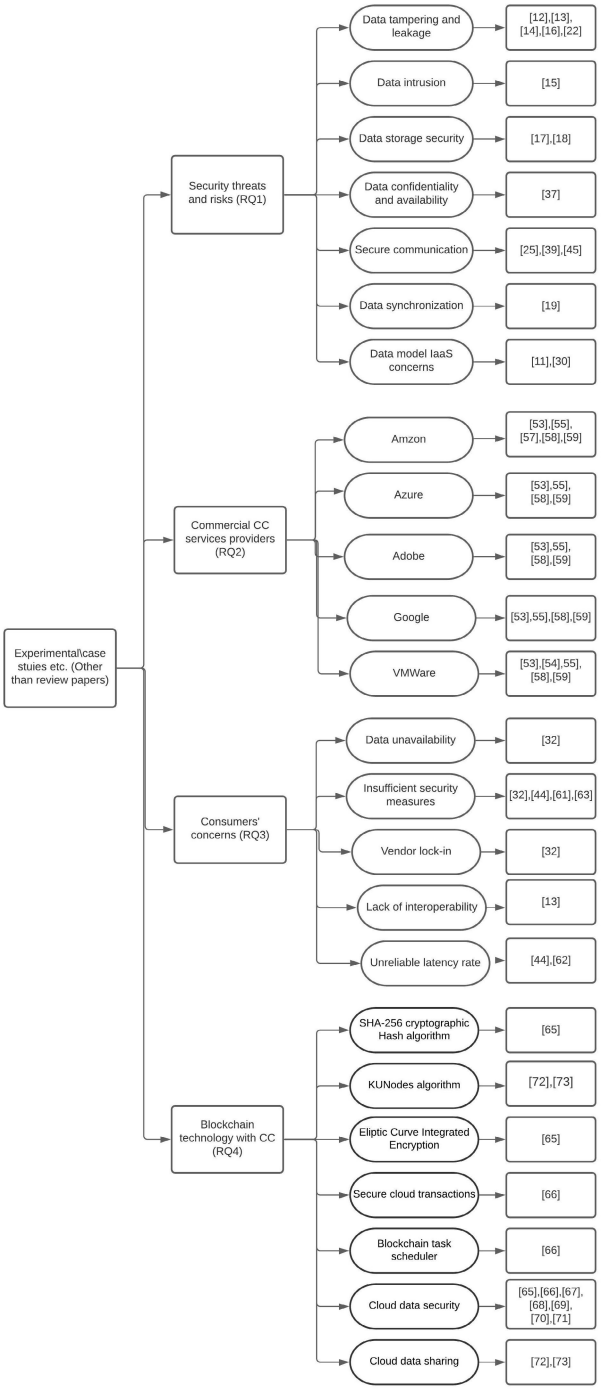

FIGURE 6. Taxonomy of studied literature to answer research questions.

to users to access the various media on different platforms. It also meets the MDB requirements and also protects sensitive information.

E. TAXONOMY DESCRIPTION

As the volume of literature is large on cloud security, it is unclear how the current research represents every class of opinion. Current research fuses some critical viewpoints of what constitutes the prominent as well as cloud security

TABLE 4. Blockchain based propsoed studies.

Research study	Problem	Proposed approach	Advantages	Disadvantages	Recommendation
[67]	Digital data security in smart city	Blockchain empowered cloud architecture	Personal information protection. Faster and secure transaction	Scalability issue in a large and scalable environment	Further extension for multiple smart city applications
[68]	Traditional health record management (traceability, security, and privacy issues)	Blockchain-based eHealth (BCE) system	Permanent storage of each transaction, such as a legitimate query	Tempered data is accountable. Need to improve the design of the proposed approach	Combining the various types of EHRs and enhance the accurate disease diagnosis
[69]	A security issue in a relational database	Identity-based proxy aggregate signature (IB-PAS) scheme	Data integrity, availability, and reliability are ensured	Compressing storage efficiency of the blockchain	Cloud may be used as an intermediate transition
[70]	Data tampering on the cloud storage	Novel public auditing schema	Defending against the malicious activities	Shows limitation in achieving a higher detection rate of malicious activities	Secure blockchain based auditing services
[71]	Consumers' distrust and high data storage cost on cloud	blockchain combined with the attribute-based signcryption	Secure data sharing on clouds	Mutual trust issue is not completely resolved	Smart contracts' deployment on ethereum
[72]	Data exchange on clouds with security and privacy	EHRs with blockchain technology	secure EHRs sharing	does show an evaluation of the proposed on various cloud	potential for using the multiple clouds
[73]	Storage sharing and access to the EMR data	an attribute-based signature scheme	unforgeable, collusion resistant and privacy-preserving	requires further evaluation remains	evaluate the large scale EMR data
[74]	Security and privacy during resource allocation	blockchain-based edge-computing framework	the edge-computing resources' effective allocation	does not show working on a public blockchain network	extension from a private to public blockchain network
[75]	An optimal resource allocation	an auction based classical algorithm	seller and buyer efficiently submit the bids	does not show an optimal resource allocation on blockchain network	resource allocation using machine learning models

challenges. This paper provides a substantial growing literature on cloud computing security challenges, commercial cloud services providers, cloud consumers' concerns, and blockchain technology. The proposed taxonomy, as shown in Fig. 6, is based on three levels. Existing literature other than the survey papers is the top one level followed by four categories on the second level. Categories at the second level are based on our proposed research questions (RQ1…RQ4). On the third level of the proposed taxonomy, we observe the different research perspectives and contributions towards answering the research question at the second level. The second level of the proposed taxonomy further highlights the challenges for category 1 (RQ1) and category (RQ3) that remain open. This taxonomy not only validates our paper's contribution; instead, it provides the opportunity for further discussion. We can extend this taxonomy by adding more categories at the second level. The fourth level of this taxonomy accounts for the focused papers on the respective categories.

F. CROSS ANALYSIS

Fig. 6 shows a taxonomic analysis and categorizes domains in a pictorial representation. A taxonomy was developed using the cloud computing security approaches. This survey paper further extends to several research directions of the proposed taxonomy (see Fig. 6). It is crucial to introspect the current approaches on cloud security, cloud security addressed by commercial cloud computing services providers, and blockchain technology. Security threats have been studied in the literature than consumers' concern (42% vs. 17%), while security techniques with blockchain technology are studies in 25% of studies. On the other hand, 17% of studies presented commercial CC service providers.

V. LIMITATIONS

This systematic literature review covers a large number of studies to answer the designed research questions. We are sure that a systematic literature review covers the cloud security issues, cloud security models, risk mitigation strategies, security issues to CSPs and users, and the role of blockchain technology, which are published to date. One of the limitations include the simplified search keywords used to search for research articles in this SLR. However, those search keywords can be further generalized. It is unnecessary that the authors of research articles were native English speakers, so there is always a risk that some terms used in research studies may be misinterpreted. However, this deficiency has been overcome by double-checking the result and discussion sections to verify English language terms' correct use. Another limitation of this SLR is excluding very recently published research studies supposed to be included in this SLR to answer the RQs but were not included.

TABLE 5. Survey papers on cloud computing topics.

Survey Paper Id	Reference
SP1	S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34, no. 1, pp. 1-11, 2011.
SP2	M. T. Khorshed, A. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation computer systems, vol. 28, no. 6, pp. 833-851, 2012.
SP3	C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The journal of supercomputing, vol. 63, no. 2, pp. 561-592, 2013.
SP4	N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," Future generation computer systems, vol. 29, no. 1, pp. 84-106, 2013.
SP5	C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, vol. 39, no. 1, pp. 47-54, 2013.
SP6	M. D. Ryan, "Cloud computing security: The scientific challenge, and a survey of solutions," Journal of Systems and Software, vol. 86, no. 9, pp. 2263-2268, 2013.
SP7	F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," Procedia Computer Science, vol. 37, pp. 357-362, 2014.
SP8	I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1-35, 2014.
SP9	J. A. González-Martínez, M. L. Bote-Lorenzo, E. Gómez-Sánchez, and R. Cano-Parra, "Cloud computing and education: A state-of-the-art survey," Computers & Education, vol. 80, pp. 132-151, 2015.
SP10	Z.-H. Zhan, X.-F. Liu, Y.-J. Gong, J. Zhang, H. S.-H. Chung, and Y. Li, "Cloud computing resource scheduling and a survey of its evolutionary approaches," ACM Computing Surveys (CSUR), vol. 47, no. 4, pp. 1-33, 2015.
SP11	Y. Wang, R. Chen, and D.-C. Wang, "A survey of mobile cloud computing applications: Perspectives and challenges," Wireless Personal Communications, vol. 80, no. 4, pp. 1607-1623, 2015.
SP12	A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," Future generation computer systems, vol. 56, pp. 684-700, 2016.
SP13	S. Singh and I. Chana, "A survey on resource scheduling in cloud computing: Issues and challenges," Journal of grid computing, vol. 14, no. 2, pp. 217-264, 2016.
SP14	J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," ACM Computing Surveys (CSUR), vol. 49, no. 1, pp. 1-39, 2016.
SP15	S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200-222, 2016.
SP16	M. A. Khan, "A survey of security issues for cloud computing," Journal of network and computer applications, vol. 71, pp. 11-29, 2016.
SP17	M. A. Nadeem, "Cloud computing: security issues and challenges," Journal of Wireless Communications, vol. 1, no. 1, pp. 10-15, 2016.
SP18	G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," Procedia Computer Science, vol. 110, pp. 465-472, 2017.
SP19	M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," Journal of Network and Computer Applications, vol. 84, pp. 38-54, 2017.
SP20	A. Ghorbel, M. Ghorbel, and M. Jmaiel, "Privacy in cloud computing environments: a survey and research challenges," The Journal of Supercomputing, vol. 73, no. 6, pp. 2763-2800, 2017.
SP21	B. Zhou and R. Buyya, "Augmentation techniques for mobile cloud computing: A taxonomy, survey, and future directions," ACM Computing Surveys (CSUR), vol. 51, no. 1, pp. 1-38, 2018.
SP22	M. Adhikari, T. Amgoth, and S. N. Srirama, "A survey on scheduling strategies for workflows in cloud environment and emerging trends," ACM Computing Surveys (CSUR), vol. 52, no. 4, pp. 1-36, 2019.
SP23	A. Arunarani, D. Manjula, and V. Sugumaran, "Task scheduling techniques in cloud computing: A literature survey," Future Generation Computer Systems, vol. 91, pp. 407-415, 2019.
SP24	P. J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," IEEE Access, vol. 7, pp. 147420-147452, 2019.
SP25	S. Pavithra, S. Ramya, and S. Prathibha, "A survey on cloud security issues and blockchain," in 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), 2019: IEEE, pp. 136-140.
SP26	D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4946-4967, 2019.
SP27	S. N. Mthunzi, E. Benkhelifa, T. Bosakowski, C. G. Guegan, and M. Barhamgi, "Cloud computing security taxonomy: From an atomistic to a holistic view," Future Generation Computer Systems, vol. 107, pp. 620-644, 2020.
SP28	H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," The journal of supercomputing, vol. 76, no. 12, pp. 9493-9532, 2020.
SP29	T. Welsh and E. Benkhelifa, "On Resilience in Cloud Computing: A survey of techniques across the Cloud Domain," ACM Computing Surveys (CSUR), vol. 53, no. 3, pp. 1-36, 2020.
SP30	P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," IEEE Access, vol. 8, pp. 131723-131740, 2020.
SP31	H. Baniata and A. Kertesz, "A survey on blockchain-fog integration approaches," IEEE Access, vol. 8, pp. 102657-102668, 2020.
SP32	A. Shakarami, M. Ghobaei-Arani, M. Masdari, and M. Hosseinzadeh, "A survey on the computation offloading approaches in mobile edge/cloud computing environment: a stochastic-based perspective," Journal of Grid Computing, pp. 1-33, 2020.
SP33	A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, "Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey," Journal of Ambient Intelligence and Humanized Computing, pp. 1-30, 2020.

VI. CONCLUSION AND FUTURE WORKS

First, in this SLR, we have reviewed the literature on cloud computing topics, including cloud security threats and their mitigation strategies. We identified several security risks to cloud computing. Data tampering and leakage is one of the identified risks. Consumers' trustworthiness, data outsourcing, and its associated risks are significant challenges identified in this SLR. This SLR identified commercial cloud services providers and highlighted the security issues they face during cloud services deployment and implementation. The trustworthiness of cloud users is challenging to consumers of commercial cloud services providers. Data unavailability, insufficient security measures, and vendor lock-in, lack of interoperability and standards are identified additionally to above-mentioned issues.

Moreover, we identified that Tweeter data generates and is used to evaluate the proposed CC approaches. This SLR identified that researchers had rarely used Facebook and Instagram data for the evaluation of proposed strategies. During the CC deployment and implementations, data security and privacy are concerns that a cloud adopting must consider before using the cloud services. Blockchain technology is found as an emerging technology to alleviate the security concerns in the CC environment.

Cloud computing services have significant advantages for vendors and users but need to bridge security gaps for cloud users. Overall, this SLR claimed that security was the most critical issue for users and CSPs. Literature review supported our claim and thus it is suggested to propose an appropriate implementation of cloud computing security policies and standards. We have presented some recommendations in Table 4, which can be practiced, and implemented in future works.

APPENDIX

See Table 5.

REFERENCES

[1] P. T. Jaeger, J. Lin, and J. M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?" *J. Inf. Technol. Politics*, vol. 5, no. 3, pp. 269–283, Oct. 2008.

[2] C. Vidal and K.-K. R. Choo, "Situational crime prevention and the mitigation of cloud computing threats," in *Proc. Int. Conf. Secur. Privacy Commun. Syst.* Springer, 2017, pp. 218–233.

[3] N. Khan and A. Al-Yasiri, "Cloud security threats and techniques to strengthen cloud computing adoption framework," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. Hershey, PA, USA: IGI Global, 2018, pp. 268–285.

[4] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system," *Computing*, vol. 98, no. 11, pp. 1111–1135, Nov. 2016.

[5] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 198–211, Jul. 2013.

[6] J.-Y. Park, S.-H. Na, and E.-N. Huh, "An optimal investment scheme based on ATM considering cloud security environment," in *Proc. 11th Int. Conf. Ubiquitous Inf. Manage. Commun.*, Jan. 2017, pp. 1–7.

[7] P. A. Boampong and L. A. Wahsheh, "Different facets of security in the cloud," in *Proc. 15th Commun. Netw. Simulation Symp.*, 2012, pp. 1–7.

[8] K. Jamsa, *Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security and More*. Burlington, MA, USA: Jones & Bartlett, 2012.

[9] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Apr. 2010, pp. 27–33.

[10] A. Bouayad, A. Blilat, N. E. H. Mejhed, and M. El Ghazi, "Cloud computing: Security challenges," in *Proc. Colloq. Inf. Sci. Technol.*, Oct. 2012, pp. 26–31.

[11] M. K. Hussein, M. H. Mousa, and M. A. Alqarni, "A placement architecture for a container as a service (CaaS) in a cloud environment," *J. Cloud Comput.*, vol. 8, no. 1, p. 7, Dec. 2019.

[12] C. S. Alliance, "Top threats to cloud computing v1. 0," Cloud Secur. Alliance, Bellingham, WA, USA, White Paper 23, 2010.

[13] S. M. Habib, S. Ries, and M. Muhlhauser, "Cloud computing landscape and research challenges regarding trust and reputation," in *Proc. 7th Int. Conf. Ubiquitous Intell. Comput. 7th Int. Conf. Autonomic Trusted Comput.*, Oct. 2010, pp. 410–415.

[14] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1097–1107, 2011.

[15] B. Halpert, *Auditing Cloud Computing*. Hoboken, NJ, USA: Wiley, 2011.

[16] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," in *Proc. IEEE 8th Int. Symp. Service Oriented Syst. Eng.*, Apr. 2014, pp. 344–351.

[17] M. A. Zardari, L. T. Jung, and M. N. B. Zakaria, "Hybrid multi-cloud data security (HMCDS) model and data classification," in *Proc. Int. Conf. Adv. Comput. Sci. Appl. Technol.*, Dec. 2013, pp. 166–171.

[18] N. Sultan and S. van de Bunt-Kokhuis, "Organisational culture and cloud computing: Coping with a disruptive innovation," *Technol. Anal. Strategic Manage.*, vol. 24, no. 2, pp. 167–179, Feb. 2012.

[19] B. Tomas and B. Vuksic, "Peer to peer distributed storage and computing cloud system," in *Proc. ITI 34th Int. Conf. Inf. Technol. Interfaces*, 2012, pp. 79–84.

[20] H. Tianfield, "Security issues in cloud computing," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Apr. 2012, pp. 1082–1089.

[21] A. Yamada, Y. Miyake, K. Takemori, A. Studer, and A. Perrig, "Intrusion detection for encrypted Web accesses," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops (AINAW)*, 2007, pp. 569–576.

[22] K.-L. Tsai, F.-Y. Leu, and J.-S. Tan, "An ECC-based secure EMR transmission system with data leakage prevention scheme," *Int. J. Comput. Math.*, vol. 93, no. 2, pp. 367–383, Feb. 2016.

[23] N. Kumar, V. Verma, and V. Saxena, "A security algorithm for online analytical processing data cube," *Int. J. Comput. Appl.*, vol. 79, no. 14, pp. 7–10, Oct. 2013.

[24] N. Tirthani and R. Ganesan, "Data security in cloud architecture based on Diffie Hellman and elliptical curve cryptography," *IACR Cryptol. ePrint Arch.*, vol. 2014, p. 49, 2014.

[25] O. Alowolodu, B. Alese, A. Adetunmbi, O. Adewale, and O. Ogundele, "Elliptic curve cryptography for securing cloud computing applications," *Int. J. Comput. Appl.*, vol. 66, no. 23, pp. 1–8, 2013.

[26] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Trans. Netw. Service Manage.*, vol. 11, no. 1, pp. 60–75, Mar. 2014.

[27] R. Farrell, "Securing the cloud—Governance, risk, and compliance issues reign supreme," *Inf. Secur. J.: Global Perspective*, vol. 19, no. 6, pp. 310–319, 2010.

[28] J. Cheng, S. Qi, W. Wang, Y. Yang, and Y. Qi, "Fast consistency auditing for massive industrial data in untrusted cloud services," in *Proc. Great Lakes Symp. VLSI*, Sep. 2020, pp. 381–386.

[29] S. S. Rizvi, T. A. Bolish, and J. R. Pfeffer, "Security evaluation of cloud service providers using third party auditors," in *Proc. 2nd Int. Conf. Internet things, Data Cloud Comput.*, Mar. 2017, pp. 1–6.

[30] S. S. Manvi and G. Krishna Shyam, "Resource management for infrastructure as a service (IaaS) in cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 41, pp. 424–440, May 2014.

[31] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[32] G. Xu, W. Yu, Z. Chen, H. Zhang, P. Moulema, X. Fu, and C. Lu, "A cloud computing based system for cyber security management," *Int. J. Parallel, Emergent Distrib. Syst.*, vol. 30, no. 1, pp. 29–45, 2015.

[33] N. Garcia, T. Alcaniz, A. González-Vidal, J. B. Bernabe, D. Rivera, and A. Skarmeta, "Distributed real-time SlowDoS attacks detection over encrypted traffic using artificial intelligence," *J. Netw. Comput. Appl.*, vol. 173, Jan. 2021, Art. no. 102871.

[34] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, and S. Linkman, "Systematic literature reviews in software engineering–a tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.
[35] *Endnote X9*. Accessed: Jan. 12, 2021. [Online]. Available: https://endnote.com
[36] J. Wen, S. Li, Z. Lin, Y. Hu, and C. Huang, "Systematic literature review of machine learning based software development effort estimation models," *Inf. Softw. Technol.*, vol. 54, no. 1, pp. 41–59, Jan. 2012.
[37] B. H. Kim, W. Huang, and D. Lie, "Unity: Secure and durable personal cloud storage," presented at the CCSW ACM Workshop Cloud Comput. Secur. Workshop, New York, NY, USA, 2012, pp. 31–36.
[38] M. Nojoumian and D. R. Stinson, "Social secret sharing in cloud computing using a new trust function," in *Proc. 10th Annu. Int. Conf. Privacy, Secur. Trust*, Washington, DC, USA, Jul. 2012, pp. 161–167.
[39] H. Eken, "Security threats and solutions in cloud computing," in *Proc. World Congr. Internet Secur. (WorldCIS-)*, London, U.K., Dec. 2013, pp. 139–143.
[40] N. Deluca. (2012). *IT Consultants*. Insight on Business Technology NSK Inc. [Online]. Available:http://blog.nskinc.com/IT-Services-Boston/bid/101166/Cloud-Security-Why-Clouds-are-Safe-and-Sound
[41] M. B. Mollah, K. R. Islam, and S. S. Islam, "Next generation of computing through cloud computing technology," presented at the Elect. Comput. Eng. (CCECE), 25th IEEE Canadian Conf., Montreal, QC Canada, 2012.
[42] GED.-i. Ltd. (2013). *Cloud Computing*. [Online]. Available: http://www.ged-i.com/—-use-case.htm#Cloudconfig1
[43] A. M. Talib, R. Atan, R. Abdullah, and M. A. A. Murad, "Security framework of cloud data storage based on multi agent system architecture: Semantic literature review," *Comput. Inf. Sci.*, vol. 3, no. 4, pp. 175–186, Oct. 2010.
[44] S. Sakr, A. Liu, D. M. Batista, and M. Alomari, "A survey of large scale data management approaches in cloud environments," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 311–336, 3rd Quart., 2011.
[45] D. C. Marinescu, *Cloud Computing: Theory and Practice*. Waltham, MA, USA: Elsevier, 2013.
[46] J. W. Bos. (2013). *Elliptic Curve Cryptography in Practice*. [Online]. Available: https://eprint.iacr.org/2013/734.pdf
[47] A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *J. Med. Syst.*, vol. 40, no. 6, p. 155, Jun. 2016.
[48] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple, and I. U. Din, "Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies," *Electronics*, vol. 9, no. 7, p. 1172, Jul. 2020.
[49] S. Shamshirband, M. Fathi, A. T. Chronopoulos, A. Montieri, F. Palumbo, and A. Pescapè, "Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102582.
[50] J. K. Samriya and N. Kumar, "A novel intrusion detection system using hybrid clustering-optimization approach in cloud computing," *Mater. Today, Proc.*, pp. 1–6, 2020, doi: 10.1016/j.matpr.2020.09.614.
[51] A. Bentajer, M. Hedabou, K. Abouelmehdi, and S. Elfezazi, "CS-IBE: A data confidentiality system in public cloud storage system," *Procedia Comput. Sci.*, vol. 141, pp. 559–564, 2018.
[52] M. Rady, T. Abdelkader, and R. Ismail, "Integrity and confidentiality in cloud outsourced data," *Ain Shams Eng. J.*, vol. 10, no. 2, pp. 275–285, Jun. 2019.
[53] M. Alshehri, "An effective mechanism for selection of a cloud service provider using cosine maximization method," *Arabian J. Sci. Eng.*, vol. 44, no. 11, pp. 9291–9300, 2019.
[54] P. Varshney and Y. Simmhan, "Characterizing application scheduling on edge, fog, and cloud computing resources," *Softw., Pract. Exper.*, vol. 50, no. 5, pp. 558–595, May 2020.
[55] H. Zhang, P. Li, Z. Zhou, J. Wu, and X. Yu, "A privacy-aware virtual machine migration framework on hybrid clouds," *J. Netw.*, vol. 9, no. 5, p. 1086, May 2014.
[56] L. Heilig, E. Lalla-Ruiz, and S. Voß, "Modeling and solving cloud service purchasing in multi-cloud environments," *Expert Syst. Appl.*, vol. 147, Jun. 2020, Art. no. 113165.
[57] C. Ngo, Y. Demchenko, and C. de Laat, "Multi-tenant attribute-based access control for cloud infrastructure services," *J. Inf. Secur. Appl.*, vols. 27–28, pp. 65–84, Apr. 2016.
[58] R. Duncan, "A multi-cloud world requires a multi-cloud security approach," *Comput. Fraud Secur.*, vol. 2020, no. 5, pp. 11–12, May 2020.
[59] B. Scott, "How a zero trust approach can help to secure your AWS environment," *Netw. Secur.*, vol. 2018, no. 3, pp. 5–8, Mar. 2018.
[60] M. Ramachandran, "Software security requirements management as an emerging cloud computing service," *Int. J. Inf. Manage.*, vol. 36, no. 4, pp. 580–590, Aug. 2016.
[61] G. Adamson, L. Wang, M. Holm, and P. Moore, "Cloud manufacturing–a critical review of recent development and future trends," *Int. J. Comput. Integr. Manuf.*, vol. 30, nos. 4–5, pp. 347–380, 2015.
[62] P. Singh, Y. K. Dwivedi, K. S. Kahlon, R. S. Sawhney, A. A. Alalwan, and N. P. Rana, "Smart monitoring and controlling of government policies using social media and cloud computing," *Inf. Syst. Frontiers*, pp. 315–337, Apr. 2019.
[63] S. Gupta, S. C. Misra, N. Kock, and D. Roubaud, "Organizational, technological and extrinsic factors in the implementation of cloud ERP in SMEs," *J. Organizational Change Manage.*, vol. 31, no. 1, pp. 83–102, Feb. 2018.
[64] A. Albugmi, R. Walters, and G. Wills, "A framework for cloud computing adoption by saudi government overseas agencies," in *Proc. 5th Int. Conf. Future Commun. Technol. (FGCT)*, Aug. 2016, pp. 1–5.
[65] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Mater. Today: Proc.*, vol. 37, pp. 2653–2659, 2021.
[66] A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on blockchain technology," *Simul. Model. Pract. Theory*, vol. 99, Feb. 2020, Art. no. 102038.
[67] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, "Blockchain-empowered cloud architecture based on secret sharing for smart city," *J. Inf. Secur. Appl.*, vol. 57, Mar. 2021, Art. no. 102686.
[68] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments," *J. Parallel Distrib. Comput.*, vol. 148, pp. 46–57, Feb. 2021.
[69] Y. Ren, Y. Leng, J. Qi, P. K. Sharma, J. Wang, Z. Almakhadmeh, and A. Tolba, "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Gener. Comput. Syst.*, vol. 115, pp. 304–313, Feb. 2021.
[70] J. Li, J. Wu, G. Jiang, and T. Srikanthan, "Blockchain-based public auditing for big data in cloud storage," *Inf. Process. Manage.*, vol. 57, no. 6, Nov. 2020, Art. no. 102382.
[71] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *J. Syst. Archit.*, vol. 102, Jan. 2020, Art. no. 101653.
[72] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-Health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.
[73] Q. Su, R. Zhang, R. Xue, and P. Li, "Revocable attribute-based signature for blockchain-based healthcare system," *IEEE Access*, vol. 8, pp. 127884–127896, 2020.
[74] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, "Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2226–2237, Feb. 2021.
[75] Z. Li, Z. Yang, and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3661–3669, Jun. 2019.
[76] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4000–4015, May 2020.
[77] S. Algarni, F. Eassa, K. Almarhabi, A. Almalaise, E. Albassam, K. Alsubhi, and M. Yamin, "Blockchain-based secured access control in an IoT system," *Appl. Sci.*, vol. 11, no. 4, p. 1772, Feb. 2021.
[78] T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the Internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and IoT based continuous glucose monitoring system for diabetes mellitus research and care," *Sensors*, vol. 19, no. 15, p. 3319, Jul. 2019.
[79] Y. Li, X. Feng, J. Xie, H. Feng, Z. Guan, and Q. Wu, "A decentralized and secure blockchain platform for open fair data trading," *Concurrency Comput., Pract. Exper.*, vol. 32, no. 7, Apr. 2020.
[80] Y. Wang, B. Rawal, and Q. Duan, "Securing big data in the cloud with integrated auditing," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2017, pp. 126–131.

BADER ALOUFFI received the Ph.D. degree. He is currently an Assistant Professor with the College of Computer and IT, Taif University. His research interests include software engineering, temporal logic, runtime verification, data science, and AI.

MUHAMMAD HASNAIN received the M.S. degree in software engineering from Abasyn University, Pakistan, in 2016. His research interests include software performance regression testing, web services scalability improvement, machine learning, and cloud computing.

ABDULLAH ALHARBI received the Ph.D. degree from the University of Technology Sydney, Australia. He is currently an Assistant Professor with the Information Technology Department, Taif University. His research interests include human–computer interaction, information systems modeling, big data, streaming data analytics, cybersecurity, and data science.

WAEL ALOSAIMI was born in Saudi Arabia, in 1979. He received the B.Sc. degree in computer engineering from King Abdulaziz University, in 2002, and the M.Sc. degree in computer systems security and the Ph.D. degree in cloud security from the University of South Wales, in 2011 and November 2016, respectively. From 2002 to 2004, he worked with Saline Water Conversion Corporation (SWCC), as an Instrument and Control Engineer. He served as a Trainer for Technical and Vocational Training Corporation (TVTC), until 2008. He joined Taif University, as a Teaching Assistant. It provides him with a scholarship to pursue his studies in the U.K. Since 2017, he has been an Assistant Professor with the Computer Engineering Department, Taif University. He has many publications in peer-reviewed conferences and journals. His research interests include cloud computing, cloud security, information security, network security, e-health security, the Internet of Things security, and data science.

HASHEM ALYAMI received the bachelor's degree in computer science from Taif University, Saudi Arabia, in 2007, the master's degree in secure computer system from the University of Hertfordshire, U.K., and the Ph.D. degree from the University of Reading, U.K. He is currently an Assistant Professor with the Computer and Information Technology College, Taif University. His research interests include cybersecurity, artificial intelligent, and data science.

MUHAMMAD AYAZ received the B.S. and M.S. degrees in computer science. He is currently pursuing the Ph.D. degree with the School of IT, Monash University, Australia. His research interests include eHealth, software engineering, databases, big data computing, and cloud computing.