JML | REVIEW

Security challenges and solutions using healthcare cloud computing

Mohammad **Mehrtak** [1], SeyedAhmad **SeyedAlinaghi** [2], Mehrzad **MohsseniPour** [2], Tayebeh **Noori** [3], Amirali **Karimi** [4], Ahmadreza **Shamsabadi** [5], Mohammad **Heydari** [6], Alireza **Barzegary** [7], Pegah **Mirzapour** [2], Mahdi **Soleymanzadeh** [8], Farzin **Vahedi** [4], Esmaeil **Mehraeen** [6]*, Omid **Dadras** [9]

Author Affiliations:

1. School of Medicine and Allied Medical Sciences, Ardabil University of Medical Sciences, Ardabil, Iran
2. Iranian Research Center for HIV/AIDS, Iranian Institute for Reduction of High Risk Behaviors, Tehran University of Medical Sciences, Tehran, Iran
3. Department of Health Information Technology, Zabol University of Medical Sciences, Zabol, Iran
4. School of medicine, Tehran University of Medical Sciences, Tehran, Iran
5. Department of Health Information Technology, Esfarayen Faculty of Medical Sciences, Esfarayen, Iran
6. Department of Health Information Technology, Khalkhal University of Medical Sciences, Khalkhal, Iran
7. School of medicine, Islamic Azad University, Tehran, Iran
8. Farabi Hospital, School of Medicine, Tehran University of Medical Sciences, Tehran, Iran
9. Department of Global Health and Socioepidemiology, Graduate School of Medicine, Kyoto University, Kyoto, Japan

***Corresponding Author:**
Esmaeil Mehraeen, Department of Health Information Technology, Khalkhal University of Medical Sciences, 1419733141, Khalkhal, Iran.
E-mail: es.mehraeen@gmail.com

DOI
10.25122/jml-2021-0100

Dates
Received: 29 May 2021
Accepted: 22 July 2021

ABSTRACT

Cloud computing is among the most beneficial solutions to digital problems. Security is one of the focal issues in cloud computing technology, and this study aims at investigating security issues of cloud computing and their probable solutions. A systematic review was performed using Scopus, Pubmed, Science Direct, and Web of Science databases. Once the title and abstract were evaluated, the quality of studies was assessed in order to choose the most relevant according to exclusion and inclusion criteria. Then, the full texts of studies selected were read thoroughly to extract the necessary results. According to the review, data security, availability, and integrity, as well as information confidentiality and network security, were the major challenges in cloud security. Further, data encryption, authentication, and classification, besides application programming interfaces (API), were security solutions to cloud infrastructure. Data encryption could be applied to store and retrieve data from the cloud in order to provide secure communication. Besides, several central challenges, which make the cloud security engineering process problematic, have been considered in this study.

KEYWORDS: health cloud, security, privacy, cloud computing, solutions, virtual network.

INTRODUCTION

Recently, clinical service demand on technology has been increased; cloud computing solutions, telemedicine, artificial intelligence, and electronic health can frequently provide better services [1]. Cloud computing is the delivery of different services through the Internet. These resources include tools and applications such as data storage, servers, databases, networking, and software [2]. Rather than owning their computing infrastructure or data centers, companies and organizations can lease access to whatever consists of storage or processing by the cloud service providers [3]. Shared resources, including servers, networks, storage tools, and application software,

use cloud computing significantly [4, 5]. Also, cloud computing users can access their programs and information using the Internet as a conduit. The adoption of cloud technology has been increased in all industries, including healthcare [6, 7].

Healthcare organizations generate a wide range of data and information. Big data in the field of health need infrastructure for better storage and management. Patient data availability is one of the most vital needs in the health and medical industry [8]. Also, health researchers need easy access to extensive data for scientific analysis. Cloud technologies are applied in healthcare fields, such as mobile apps, patient portals, electronic medical records, devices with the Internet of Things (IoT), and big data analytics [9–11)] As per the service demands, healthcare providers need considerably to scale the data storage and network requirements.

Furthermore, using the cloud in electronic health records enables patients to easily and widely access their health information. Cloud computing changes how nurses, doctors, hospitals, and clinics deliver quality and profitable services to the patients. The challenges in the healthcare field include operational and infrastructure costs, security concerns to real-time information sharing, and robust backup.

Cloud computing has several advantages, including easy and convenient collaboration between users, reduced costs, increased speed, scalability, and flexibility. The data sharing process is more facilitated by cloud computing. Further, it has the potential to significantly decrease in-house infrastructural and operational costs in healthcare organizations [15]. By changing traditional data storage and handling procedures, cloud technology can speed up access to information and overcome the barriers that the industry stakeholders and patients encounter. Despite the numerous benefits of cloud computing, there are some drawbacks and challenges. Healthcare organizations are hesitant to adopt cloud computing due to security concerns, including patient information confidentiality, privacy, and service costs [16, 17]. Although massive data generated in healthcare organizations should be available to physicians and researchers, confidentiality concerns must be considered [18–20]. New challenges in cloud computing technology emerge in tandem with the growth, epiphany, and use of cloud technology in healthcare organizations; thus, identifying healthcare challenges and security issues appears essential. Accordingly, there are new challenges or security issues concerning offered solutions to cloud computing in healthcare organizations that should be examined and reviewed. Alongside identifying security challenges in cloud technology, reviewing present security solutions and providing new ones are also important objectives of this study. The present study aims at identifying barriers, challenges, security issues, and solutions in implementing cloud computing in the healthcare industry.

MATERIAL AND METHODS

Design

As this systematic review aimed at updating the results of earlier studies [21] concerning the topic, the eligible articles from the beginning of 2015 to November 2020 were retrieved. A comprehensive search of relevant literature was conducted utilizing the online databases of Scopus, Pubmed, Science Direct, and Web of Science. Two researchers were involved in the online search and identification of the relevant articles. In the first step, based on the inclusion criteria, the relevant studies were included using relevant keywords in the title or abstract. The literature not relevant to the present research and those with no original data were excluded. The second step involved a scrutinized full-text screening of the related article to choose the most eligible.

Research question

This study aims to address the following issues of the modern healthcare systems:
- What are the main challenges threatening the security of cloud computing?
- What are the solutions to overcome these potential difficulties?

Inclusion/Exclusion criteria

We included the English studies serving our study's purpose from the beginning of 2015 to November 2020.
The exclusion criteria were as follows:
- Preliminary data from incompleted projects;
- Abstracts, conference abstracts, and any other incomplete projects without full-text manuscripts;
- Review articles, letters to the editors, or any types of articles lacking original data.
- Articles lacking available free full-text.

RESULTS

A total of 930 full texts of related studies were identified using the selected search strategy. After reviewing them, 360 duplicates were identified and removed; then, two independent investigators screened the title and abstract of the rest (570 resources). The full text of

the extracted articles was reviewed, and the most relevant (245 resources) were selected based on the eligibility criteria. According to the selection criteria, 197 articles were excluded, all of which were found to be reviews (n=36), opinion articles (n=28), or not involving cloud security (n=133). Finally, 48 studies met inclusion criteria and were included in the final review (Figure 1).

We identified common security challenges and potential solutions for cloud technology. The reviewed studies and cloud computing security challenges and solutions are presented in Table 1. According to the review of the studies, the most frequent cloud security challenges were information confidentiality (n=19), data security (n=14), data availability (n=14), data integrity (n=13), and network security (n=12); frequency data are shown in Figure 2. Furthermore, data encryption (n=17), authentication (n=10), application programming interfaces (API)(n=7), and data classification (n=6) were the most common solutions for the security challenges in cloud infrastructure (Figure 3).

DISCUSSION

Although cloud computing, as a novel technology, provides patient data availability all across, it encounters critical challenges in meeting one of the health industry's most significant demands. In cloud computing, providing security systems is necessary due to its inherent features, such as remote data storage, lack of network environment, proliferation, and massive infrastructure sharing [69]. Therefore, accurate identification of security challenges and their appropriate solutions is essential for both cloud computing providers and organizations using this technology [62].

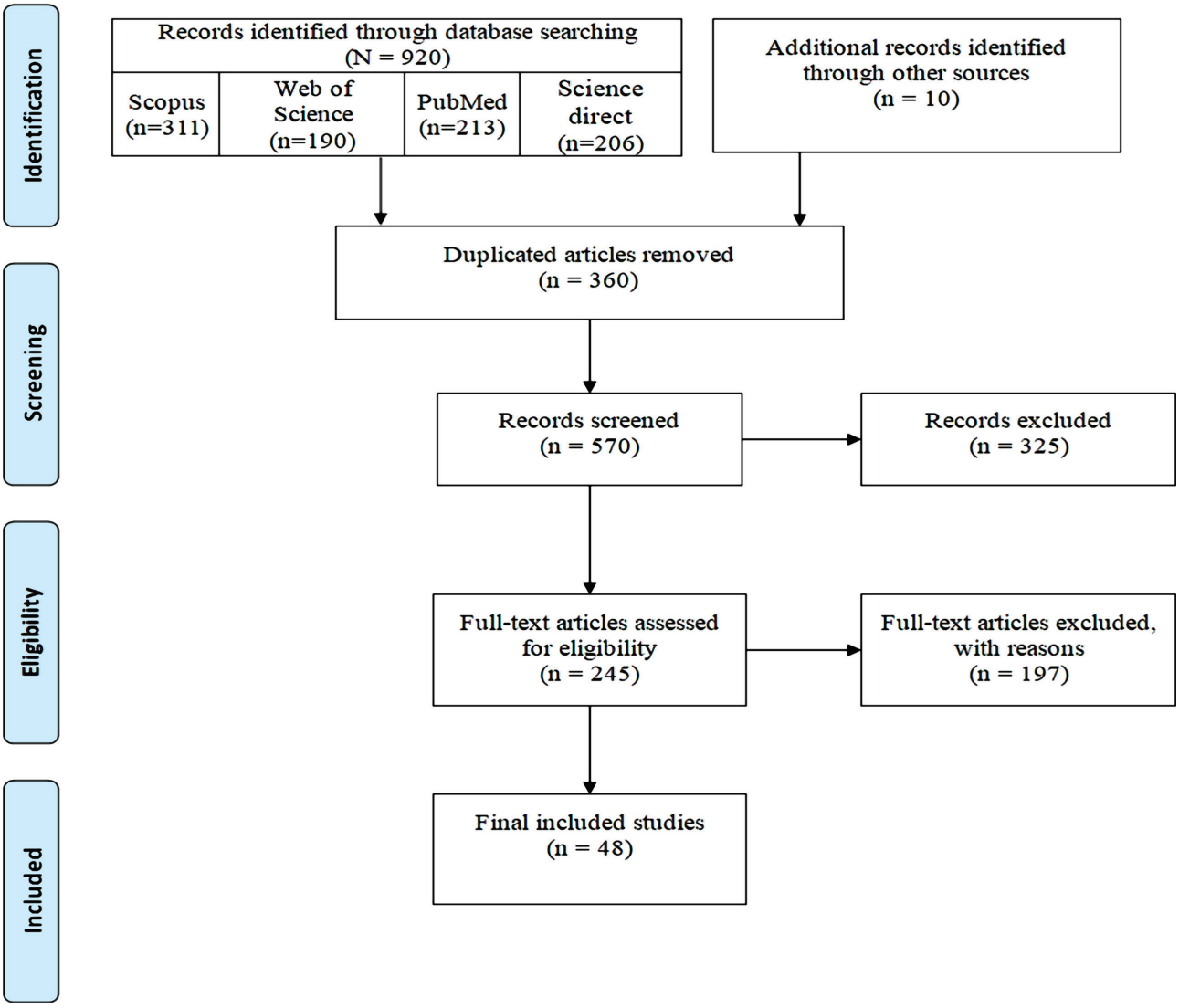

Figure 1. Flow diagram for the selection process of identified articles.

Table 1. Identified security challenges and potential solutions in healthcare cloud computing.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
1	Dashti W [22]	2020	Pakistan	Security challenges in cloud computing	Availability, confidentiality, data integrity, control, audit, virtual machine security, network security	--
2	Ogiela L [23]	2020	Poland	Intelligent data management and security in cloud computing	Techniques of secret data management and protection	Cryptographic threshold techniques applied to split the secret in a specified group of trustees, being enhanced simultaneously using the shared secret intelligent linguistic threshold schemes
3	Tariq MI [24]	2020	Pakistan	Information security controls via Fuzzy AHP for cloud computing and wireless sensor networks	The proportionate security of networks	Fuzzy Analytical Hierarchy Process (FAHP); Analytical Hierarchy Process (AHP); Fuzzy AHP Methodology.
4	Tabrizchi H [20]	2020	Iran	Security challenges in cloud computing	Security policies, user-oriented security, application security, data storage, network	Data encryption (cryptography, quantum cryptography), secure sockets layer (SSL); Hash functions, message signature, message authentication code; Intrusion detection and prevention systems; firewalls, packet filters; Digital signature, endorsing certificate, notary; public and private blockchains
5	Wu B [25]	2020	China	Security and secure channel	Strategies to assure the confidentiality and security of outsourced sensitive data	Channel-free certificate less searchable public-key authenticated encryption (dCLPAEKS) scheme
6	Shakil KA[26]	2020	India	Healthcare management system	Identity theft, tax fraudulence, medical fraud, bank fraud, insurance fraud, and defamation of high-profile patients; Extending the capabilities of health applications over mobile devices, such as tablets, laptops, and smartphones.	Biometric-based authentication mechanism; BAMHealthCloud ensures the security of e-medical data access through a behavioral; Training of the signature samples for authentication purposes has been performed in parallel on the Hadoop MapReduce framework using Resilient Backpropagation neural; ALGO Health Security that performs security checks using parallelized MapReduce programming model.
7	George Amalarethinam DI [26]	2019	India	Cloud security challenges and solutions	Availability, confidentiality, privacy, integrity	Data encryption; OTP, digital certificate, and biometric verification; Rain-6 and digital signature.
8	Giri S [28]	2019	Nepal	Cloud security challenges and solutions	Data access and confidentiality	Data encryption and classification
9	Al-Issa Y [29]	2019	Jordan	Security challenges in eHealth cloud computing	Confidentiality, integrity, availability, ownership, and privacy of healthcare information; Authenticity, non-repudiation, audit, access control, data remanence and freshness, anonymity, unlinkability cloud multitenancy, secure transmission	HIPAA, HITECH ISO/IEC 27000-Series EU General Data Protection Regulation (GDPR) Patient-Centric Approach, Encryption Techniques

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
10	Bazm MM [30]	2019	France	Virtualization layer isolation challenges	Memory deduplication; large-page memory management, non-privileged access to hardware instructions.	Detection, countermeasure, application-level, OS-level, hypervisor-level, hardware-level, and moving target defense approaches
11	Modi KJ [31]	2019	India	Cloud security challenges and solutions	Security of data is a major factor, which restricts the acceptance of the cloud-based model.	Using linear network coding and re-encryption based on ElGamal cryptography in the form of a hybrid approach to secure healthcare information over the cloud; Linear network coding mechanism.
12	Kumar PR [32]	2018	Brunei	Cloud security challenges and solutions	Confidentiality, integrity, availability, authentication, authorization, non-repudiation	Creating the data, classifying the data, identifying the sensitive data, defining policies, and creating access methods for different data types; Creating policies for archiving and destroying data; Storing data with proper physical and logical security protection, including backup and recovery plan; Identifying which datatype can be shared, with whom and how it can be shared; defining data sharing policies; In cloud computing, many such policies are collectively called as Service Level Agreements (SLA); Creating a corrective action plan in case data is corrupted or hacked due to network or communication devices; security flaws while data is in transit; Data encryption; Using data duplication, redundancy, backups, and resilient systems to address availability issues.
13	Basu S [33]	2018	India	Security challenges in cloud computing	Confidentiality, integrity, availability	--
14	Pinheiro A [34]	2018	Brazil	Security architecture and protocol for trust verifications concerning the integrity of stored files in cloud services	Organizing a cloud storage service (CSS) that is safe from the client point of view, implementing CSS in public clouds, integrity, availability, privacy, and trust for the adopting cloud storage service	
15	Subramanian N [35]	2018	India	Security challenges in cloud computing	Cloud computing threats and risks, security in crypto-cloud	Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, Testing-as-a-Service, Security-as-a-Service, Database-as-a-Service
16	Stergiou C [36]	2018	Greece	Security, privacy, and efficiency of sustainable cloud computing for big data and IoT	The security and privacy	Installing a security "wall" between the cloud server and the Internet

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
17	Abrar H [37]	2018	Pakistan	Risk analysis of cloud sourcing in healthcare and public health industry	Data breaches, data loss, account hijacking, insecure interfaces and APIs, denial-of-service attacks (dos), malicious insiders, abuse of cloud resources, insufficient due diligence, shared technology issues	Likelihood determination, impact analysis, risk determination
18	Esposito C [38]	2018	Italy	Cloud security challenges and solutions	Confidentiality, privacy	Data encryption, blockchain
19	Huang Q [39]	2018	China	Data security challenges and solutions	Confidentiality, availability	Data encryption, public-key encryption, identity-based encryption, identity-based broadcast encryption, attribute-based encryption
20	Roy S [40]	2018	India	Cloud security challenges and solutions	The authentication process and security	A combined approach of fine-grained access control over cloud-based multi-server data along with a provably secure mobile user authentication mechanism for the Healthcare Industry 4.0.
21	Al-Shqeerat KH [41]	2017	Saudi Arabia	Security challenges in cloud computing	Network security, access control, cloud infrastructure, data security	Educating the stakeholders adequately on the cloud; Making sure that the IT administrator is able to control and manage cloud items and services when concluding the contract agreement with the service provider; An agreement with a third party to perform audits regularly to monitor the performance and compliance of the service provider to the agreed terms; Monitoring the performance of available cloud services and resources periodically; Data and applications in the cloud environment must be classified based on their values (according to their importance and sensitivity); not all data stored in the cloud are rated as top secure data; Backup and recovery; Proper authentication, authorization, and access security tools and mechanisms; Providing suite strong encryption protocols and key management for data at rest, in transit, and on the backup state
22	Barona R [42]	2017	India	Security challenges in cloud computing	Data breach, account or service traffic hijacking, insecure interfaces and Application Programming Interfaces (APIs), denial-of-Service (DOS), malicious insiders, abuse of cloud services, shared technology vulnerabilities	Information-centric security,high-assurance remote server attestation privacy-enhanced business intelligence, privacy and data protection, homomorphic encryption Searchable/ structured encryption, proofs of storage, server aided secure computation
23	Bhushan K [43]	2017	India	Security challenges in cloud computing	Physical level security issues, application and software-related security issues, network-related security issues, data-related security issues, computation-related issues, hardware virtualization-related issues, management and account control-related issues, trust-related issues, compliance and law-related issues	Classification based on the type technique used, classification based on the attack detection principle, classification based on reaction time, classification based on deployment point, classification based on the degree of deployment, classification based on the degree of cooperation, classification based on the defense activity, classification based on response strategy

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
24	Park J [44]	2017	Korea	Blockchain security in cloud computing	adapting blockchain security computing and its secure solutions	Blockchain provides security through the authentication of peers that share virtual cash, encryption, and generation of the hash value
25	Radwan T [45]	2017	Egypt	Cloud computing security	Privileged access, Data location; Availability, Investigation support; Regulatory compliance, Data segregation; Recovery, Long-term viability.	Authentication, authorization
26	Singh A [46]	2017	India	Cloud security issues	Zombie attack (DoS/DDoS attack); Service injection attack; Attack on virtualization/hypervisor; User to root attacks; Port scanning; Man-in-middle attack; Metadata spoofing attack; Phishing attack; Backdoor channel attack.	Strong authentication and authorization; Strong isolation mechanisms between VMs; Using the hash function to check service integrity; web service security; Adopting secure web browsers and API; Using a strong password; better authentication mechanism; Requiring strong port security, Requiring a proper Secure Socket Layer (SSL) architecture; Service functionality and other details should be kept in encrypted form to access the file required a strong authentication mechanism; Using a secure web link (HTTPS); Requiring strong authentication, authentication, and isolation mechanisms.
27	Mohit P [47]	2017	India	Cloud security challenges and solutions	Security protection is important for medical records (data) of the patients because of very sensitive information. Patient anonymity.	Authentication protocol for TMIS using the concept of cloud environment
28	Hussein NH [48]	2016	Sudan	Cloud security challenges and solutions	Authentication and authorization; Data confidentiality; Availability; Information security; Data access; Data breaches.	Logical network segmentation; Firewalls implementing; Traffic encryption; Network monitoring;
29	Kaur M [49]	2016	India	Cloud security challenges and solutions	Confidentiality; Authentication; Integrity; Non-repudiation; Availability	Data classification; Data Encryption
30	Muthurajan V [50]	2016	India	An elliptic curve-based Schnorrcloud security model in a distributed environment	The security upgrade in data transmission Approaches	A virtual machine-based cloud model with Hybrid Cloud Security Algorithm (HCSA); The combination of Elliptic Curve-based Schnorr (EC-Schnorr) scheme and blooming filter; A virtual machine-based cloud model with Hybrid Cloud Security Algorithm (HCSA); The optimization in the computational steps by ECC signature set and the duplication removal by blooming filter in the proposed Hybrid Cloud Security Algorithm (HCSA)
31	Prakash C [51]	2016	India	Cloud computing security	Deployment model issue, service model issues, network issues	Categorization of the data according to the risk associated with the data; Service Level Agreement (SLA); isolation amongst the resources by using segmentation; development of the dedicated application; a strong two-factor authentication

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
32	Vurukonda N [52]	2016	India	Privacy and confidentiality in the cloud environment	Data privacy and integrity, improper media sanitization, data recovery and vulnerability, data backup, service level agreements malicious insider, outside intruder, legal issues, confidentiality	SecCloud, for securing cloud data; FADE, a protocol for data privacy and integrity; TimePRE, a scheme for secure data sharing in the cloud; a methodology for security of resident data SPICE, identity management framework;role-based access control scheme, identity management framework
33	Alasmari S [53]	2016	USA	Security and privacy, challenges in IoT-based health cloud	Managing credentials and controlling access to applications and patient's confidential information, implementing and deploying cryptographic protocols in IoT health cloud correctly, mitigating device vulnerabilities and deploying firmware patches, securing IoT health networks and minimizing the risk of data loss	
34	Albuquerque SL [54]	2016	Brazil	Security in cloud-computing-based mobile health	Personal equipment vulnerabilities, assurance of cloud computing service availability assurance of confidentiality and integrity in unreliable cloud environments, access control and authenticity guarantee of systems users	
35	Casola V [55]	2016	Italy	Healthcare-related data in the cloud: challenges and opportunities	Having a decentralized and distributed design, allowing asynchronous interactions, supporting security mechanisms concerning privacy regulations, providing flexible data and service integration	Cryptographic solutions, such as privacy-preserving cloud ones
36	EL Bouchti A [56]	2016	Morocco	Cloud security challenges and solutions	Confidentiality, availability, data portability	Data encryption
37	Dorairaj SD [57]	2015	India	Cloud security challenges and solutions	Confidentiality, auditability	Access control, data encryption, integrity verification, log analysis, data classification
38	Kene SG [58]	2015	India	Cloud security challenges and solutions	Confidentiality, integrity availability	Hybrid detection technique, network intrusion detection system (NIDS)
39	Liu Y [59]	2015	USA	Cloud security challenges and solutions	Loss of control, lack of transparency, multi-tenancy	Data encryption, access control

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
40	Ali M [60]	2015	USA	Security challenges in cloud computing	Communication, architectural contractual and legal mobile application security, authentication, user privacy, data security	Using virtual LANs, IPS, IDS, and firewalls as a combination to protect the data in transit; Using off-the-shelf technology; Using standard algorithms; The implementers should secure each virtualized OS in each guest VM; The VMs at rest should be encrypted; Third-party security technology should be applied to decrease dependency on the CSP; VM images at rest should be patched with the latest fixes as soon as required; Security's vulnerability assessment tools should cover the virtualized environment; Virtualization-aware security tools should be implemented and used in the cloud computing environment; The protection mechanism should be in place until VMs are patched. The risk and attack models should be continuously built and maintained; Regular penetration testing for web applications should be carried out; The secure software lifecycle and software architecture should be developed and maintained; The source of the attributes should be as close to the master one as possible; Open standard federations, such as SAML and OAuth, should be preferred if possible; Bi-directional trust should be ensured for secure relationship and transactions.
41	Anand P [61]	2015	USA	Security challenges in cloud computing	Traffic hijacking, data breaches, data loss, insecure APIs, denial-of-Service, abuse of cloud services, malicious insiders, shared technology issues	--
42	Rao RV [62]	2015	India	Data security challenges in cloud computing	Integrity, confidentiality breaches, segregation, storage, data center operation	Encryption, RSA signature,identity-based cryptography, data security RSA-based storage security technique, distributed access control architecture
43	Wang B [63]	2015	USA	DDoS attack protection	Network security	The SDN-based network management, DaMask

Table 1. Continued.

ID	The first author (reference)	Publication date	Country	Study Context	Security challenges	Solutions recommended
44	Wang Y [64]	2015	Japan	Fog computing: security and forensics	Trust issue due to dependency on CSP, preserving the integrity, decentralization of logs, absence of critical information in logs, logs in multiple tiers and layers, volatility of logs, dependency on CSP for logs, dependability on CSP for data acquisition, trust issues of cloud computing, multi-tenancy, the chain of custody	API provided by CSP for logs, the cloud management plan, robust SLA, global unity, virtual machine introspection, the trusted third party, continuous synchronization, TPM, data provenance in the cloud, isolating a cloud instance
45	Moosavi SR [65]	2015	Finland	Cloud security challenges and solutions	End-to-end security for healthcare IoT	Session resumption-based end-to-end security scheme for healthcare Internet of things (IoT), The projected scheme is realized by using a certificate-based DTLS handshake between end-users and smart gateways, besides applying the DTLS session resumption method.
46	Zhang K [66]	2015	USA	Cloud security challenges and solutions	Security and privacy	Privacy-preserving health data aggregation, secure health data access and processing, misbehavior detection for the health-oriented mobile social network application
47	Zhou J [67]	2015	China	Cloud security challenges and solutions	E-healthcare cloud computing systems	Traceable and revocable multi-authority attribute-based encryption named TR-MABE to achieve efficiently multi-level privacy preservation without introducing other special signatures, secret keys used to protect patient's identity and PHI
48	Khattak HAK [68]	2015	Pakistan	Security concerns of cloud-based healthcare systems	Confidentiality, integrity, availability, privacy	Access control, multi-cloud computing security

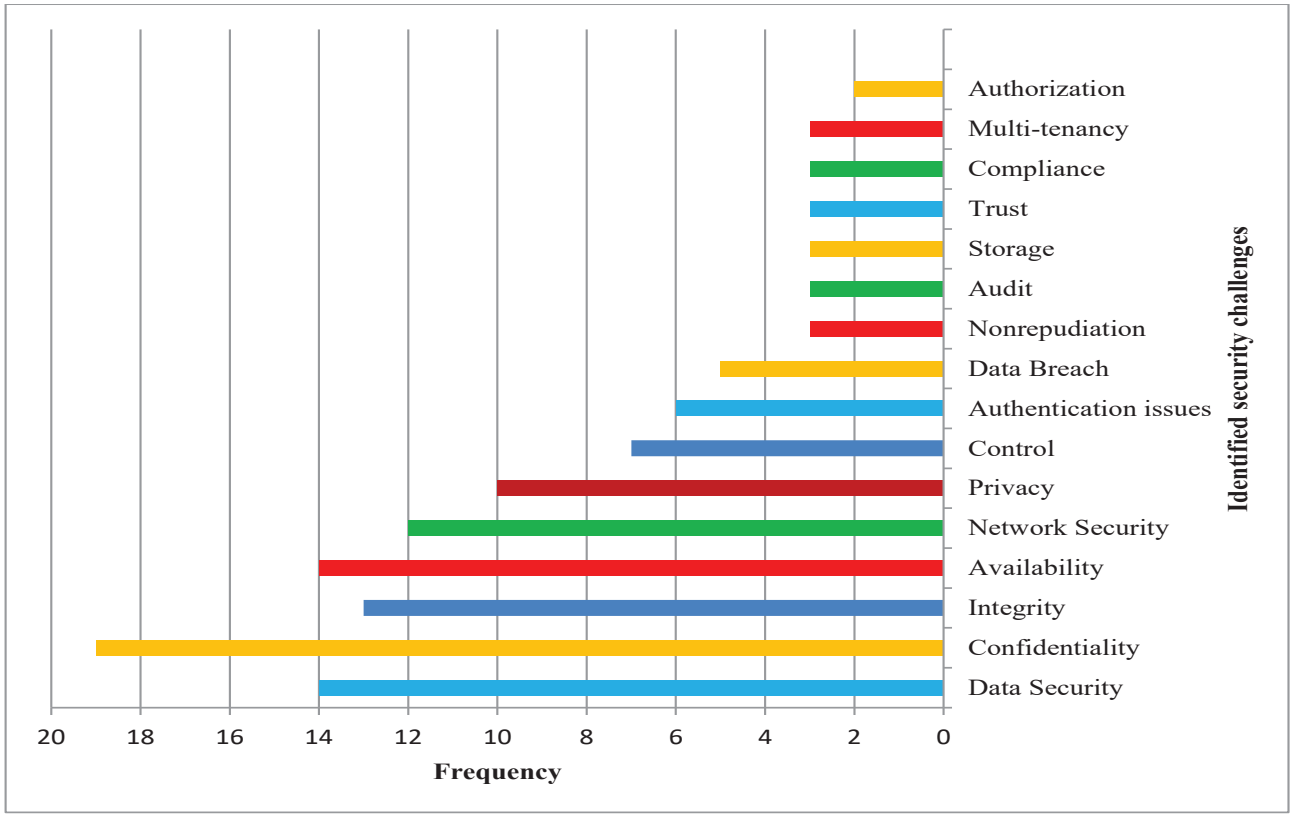

Figure 2. Frequency of the cloud computing security challenges.

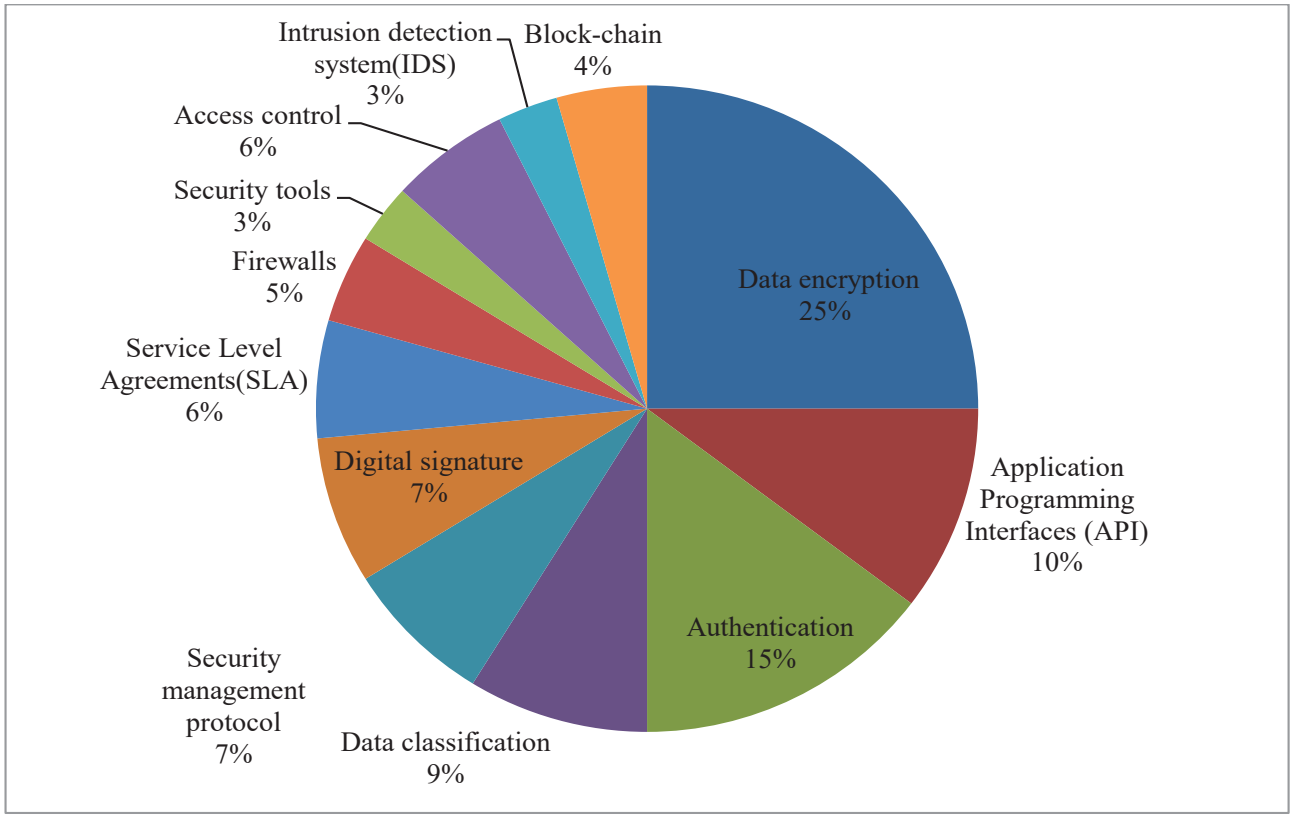

Figure 3. Most common identified solutions for security challenges in cloud computing.

Recently, artificial intelligence (AI) has shown a promising bright future in medical issues, especially when combined with cloud computing. Ahmed Sedik *et al.* have used AI deep learning to create a tool for quick screening of COVID-19 patients from their chest X-rays. This modality can be performed through a cloud-based system anywhere radiography equipment is found [70].

Identification systems also can use cloud computing. Alsmirat *et al.* have shown that digital cameras can act as a fingerprint identification system with an image compression rate of 30–40%, widely available on smartphones. Data security is a significant challenge there as well [71].

The present study indicates that the most vital challenge in cloud computing technology is maintaining data security. Malicious or negligent individuals may threaten data security. Several solutions provide data security, the most important of which is data encryption [20, 25, 29]. Data encryption is an essential line of protection in cybersecurity architecture. Encryption makes interrupted data use as difficult as possible [27, 28, 32]. Furthermore, data encryption is used to develop an encryption scheme that hypothetically can merely be broken with large amounts of computing potency [41, 42, 44, 49]. Kaur *et al.* [49] and Dorairaj *et al.* [57] have stated data encryption as a strategy to protect data against security threats. The results of the current research further show data encryption as the best solution to provide data security.

Many methods have been proposed for data encryption. A four-image encryption scheme has been proposed by Yu *et al.* based on the computer-generated hologram, quaternion fresnel transforms (QFST), and two-dimensional (2D) logistic-adjusted-sine map (LASM). This innovative technology considerably decreases the key data sent to the receiver for decryption, making it more promising to be stored and transmitted [72]. In order to secure cloud data storage and its delivery to authorized users, a hierarchal identity-based cryptography method has been proposed by Kaushik *et al.* to assure that a malicious attacker or CSP does not change for its benefit [73].

Another research has proposed a method to avoid always using the upstream communication channel from the clients to the cloud server via an optimistic concurrency control protocol, which reduces communication delay for IoT users. Only update transactions are sent to the cloud using this method, and they are only partially validated at the fog node [74].

According to the present research results, confidentiality is the second most important challenge in cloud technology. It refers to the protection of data from being obtained by unauthorized individuals; in other words, sensitive information is only accessible by authorized persons [75]. Cloud data control can result in an increased risk of data compromise. To ensure that the patient-doctor relationship runs smoothly, patients must have faith in the healthcare system to keep their data private [17]. Studies have shown that confidentiality may be achieved by access control [52, 62] and authentication [45, 76]. A Mutual Authentication and Secret Key (MASK) establishment protocol has been presented by Masud *et al.* in the field of the Internet of Medical Things (IoMT) in COVID-19 patients. The proposed protocol uses Physical Unclonable Functions (PUF) to enable the network devices to validate the doctor legitimacy (user) and sensor node before establishing a session key. Therefore, it addresses the confidentiality, authentication, and integrity problems and secures the sensitive health information of the patients [77].

This research shows that integrity, availability, and network security are important issues in the cloud computing infrastructure. A developmental study has mentioned integrity and availability as challenging problems in implementing cloud-based services, especially when losing or leaking information could result in major legal- or business-related damage [34]. Confidentiality, Integrity, and Availability (CIA) have been reported as the main three factors in cloud system security, which are considered here for the evaluation [33].

The number of network security challenges has rapidly increased with the advent of wireless sensor networks [22, 24]. Therefore, network security in cloud infrastructure has become a challenge for organizations [41, 43]. The common network attacks have happened at the network layer, including IP spoofing, port scanning, man-in-middle attack, address resolution protocol (ARP) spoofing, routing information protocol (RIP) attack, denial of service (DoS), and distributed denial of service (DDoS) [58]. The attackers, for instance, can send a considerable number of requests in order to access virtual machines in cloud computing to restrict their availability to valid users; this is termed the DoS attack. The availability of cloud resources is targeted by this attack [63]. The related studies have shown that no specific security standard exists for security controls in wireless networks [24, 51, 63]. However, in order to keep security in cloud computing networks, potential solutions, including Application Programming Interfaces (API), data classification, and security management protocol, could be applied [60, 64, 78, 79].

Limitations

Due to the nature of the solution protocols, we could not explain their details. We aimed to clarify the present challenges and possible solutions to help others address and work on the issues, thus skipping some details and protocols presented for solutions. We only reviewed the English studies, thus possibly missing some reports.

CONCLUSION

Cloud computing offers various benefits in data access and storage, particularly to healthcare organizations and relevant studies. Although the cloud computing environment is considered as a potential Internet-based computing platform, the security concerns

encountered are notable. Security concerns may occur as a result of the cloud computing paradigm's shared, virtualized, and public nature. Overcoming these challenges by developing novel solutions is the only option for cloud computing adoption. All users, individuals or organizations, should be well informed of the security risks in the cloud.

In this study, an overview of cloud computing is presented; also, its security challenges and solutions surfaced within the past five years are reviewed. In order to offer safe data access, data encryption can be utilized to store and retrieve data from the cloud. We have also gone through some of the major challenges that make cloud security engineering tough. Identifying these challenges is the first step to tackle them, and future studies need to provide more feasible solutions to fix such bugs.

ACKNOWLEDGMENTS

The present study was extracted from the research project with the IR.KHALUMS.REC.1400.001 code entitled "Investigating the necessary infrastructure for implementing cloud computing technology in Khalkhal University of Medical Sciences" conducted at the Khalkhal University of Medical Sciences in 2021.

Conflict of interest

The authors declare that there is no conflict of interest.

REFERENCES

1. Tahir A, Chen F, Khan HU, Ming Z, Ahmad A, Nazir S, *et al.* A Systematic Review on Cloud Storage Mechanisms Concerning e-Healthcare Systems. Sensors (Basel, Switzerland). 2020;20(18).

2. Whaiduzzaman M, Gani A, Anuar NB, Shiraz M, Haque MN, Haque IT. Cloud service selection using multicriteria decision analysis. TheScientificWorldJournal. 2014;2014:459375.

3. Kuo MH, Kushniruk A, Borycki E. Can cloud computing benefit health services? - a SWOT analysis. Studies in health technology and informatics. 2011;169:379-83.

4. Chow F, Muftu A, Shorter R. Virtualization and cloud computing in dentistry. Journal of the Massachusetts Dental Society. 2014;63(1):14-7.

5. Mayfield CA, Gigler ME, Snapper L, Jose J, Tynan J, Scott VC, *et al.* Using cloud-based, open-source technology to evaluate, improve, and rapidly disseminate community-based intervention data. Journal of the American Medical Informatics Association : JAMIA. 2020.

6. Kuo AM. Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research. 2011;13(3):e67.

7. Pechette JM. Transforming health care through cloud computing. Health care law monthly. 2012;2012(5):2-12.

8. Yao Q, Han X, Ma XK, Xue YF, Chen YJ, Li JS. Cloud-based hospital information system as a service for grassroots healthcare institutions. Journal of medical systems. 2014;38(9):104.

9. Griebel L, Prokosch HU, Köpcke F, Toddenroth D, Christoph J, Leb I, *et al.* A scoping review of cloud computing in healthcare. BMC medical informatics and decision making. 2015;15:17.

10. Sadoughi F, Erfannia L. Health Information System in a Cloud Computing Context. Studies in health technology and informatics. 2017;236:290-7.

11. Madanian S, Parry D. IoT, Cloud Computing and Big Data: Integrated Framework for Healthcare in Disasters. Studies in health technology and informatics. 2019;264:998-1002.

12. Wang Y, Tian Y, Tian LL, Qian YM, Li JS. An electronic medical record system with treatment recommendations based on patient similarity. Journal of medical systems. 2015;39(5):55.

13. Ahmadi M, Aslani N. Capabilities and Advantages of Cloud Computing in the Implementation of Electronic Health Record. Acta informatica medica : AIM : journal of the Society for Medical Informatics of Bosnia & Herzegovina : casopis Drustva za medicinsku informatiku BiH. 2018;26(1):24-8.

14. Kim M, Yu S, Lee J, Park Y, Park Y. Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. Sensors (Basel, Switzerland). 2020;20(10).

15. Mrozek D. A review of Cloud computing technologies for comprehensive microRNA analyses. Computational biology and chemistry. 2020;88:107365.

16. Sajid A, Abbas H. Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges. Journal of medical systems. 2016;40(6):155.

17. Al-Issa Y, Ottom MA, Tamrawi A. eHealth Cloud Security Challenges: A Survey. J Healthc Eng. 2019;2019:7516035.

18. Behl A, editor Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. 2011 World Congress on Information and Communication Technologies; 2011: IEEE.

19. Moura J, Hutchison D. Review and analysis of networking challenges in cloud computing. Journal of Network and Computer Applications. 2016;60:113-29.

20. Tabrizchi H, Rafsanjani MK. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing. 2020:1-40.

21. Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari SJGJoHS. Security challenges in healthcare cloud computing: a systematic review. 2016;9(3):157.

22. Dashti W, Qureshi A, Jahangeer A, Zafar A. Security challenges over cloud environment from service provider prospective. Cloud Computing and Data Science. 2020:12-20.

23. Ogiela L, Ogiela MR, Ko H. Intelligent Data Management and Security in Cloud Computing. Sensors (Basel, Switzerland). 2020;20(12).

24. Tariq MI, Ahmed S, Memon NA, Tayyaba S, Ashraf MW, Nazir M, *et al.* Prioritization of Information Security Controls through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks. Sensors (Basel, Switzerland). 2020;20(5).

25. Wu B, Wang C, Yao H. Security analysis and secure channel-free certificateless searchable public key authenticated encryption for a cloud-based Internet of things. PloS one. 2020;15(4):e0230722.

26. Shakil KA, Zareen FJ, Alam M, Jabin S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University-Computer and Information Sciences. 2020;32(1):57-64.

27. George Amalarethinam D, Rajakumari S. A Survey on Security Challenges in Cloud Computing. 2019.

28. Giri S, Shakya S. Cloud Computing and Data Security Challenges: A Nepal Case. International Journal of Engineering Trends and Technology, 67 (3), 146. 2019;150.

29. Al-Issa Y, Ottom MA, Tamrawi A. eHealth cloud security challenges: A survey. Journal of Healthcare Engineering. 2019;2019.

30. Bazm M-M, Lacoste M, Südholt M, Menaud J-M. Isolation in cloud computing infrastructures: new security challenges. Annals of Telecommunications. 2019;74(3):197-209.

31. Modi KJ, Kapadia N. Securing healthcare information over cloud using hybrid approach. Progress in advanced computing and intelligent engineering: Springer; 2019. p. 63-74.

32. Kumar PR, Raj PH, Jelciana P. Exploring data security issues and solutions in cloud computing. Procedia Computer Science. 2018;125:691-7.

33. Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M, *et al.*, editors. Cloud computing security challenges & solutions-A survey. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC); 2018: IEEE.

34. Pinheiro A, Dias Canedo E, de Sousa Junior RT, de Oliveira Albuquerque R, García Villalba LJ, Kim TH. Security Architecture and Protocol for Trust Verifications Regarding the Integrity of Files Stored in Cloud Services. Sensors (Basel, Switzerland). 2018;18(3).

35. Subramanian N, Jeyaraj A. Recent security challenges in cloud computing. Computers & Electrical Engineering. 2018;71:28-42.

36. Stergiou C, Psannis K, Gupta B, Ishibashi Y. Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT. Sustain Comput Informatics Syst. 2018;19:174-84.

37. Abrar H, Hussain SJ, Chaudhry J, Saleem K, Orgun MA, Al-Muhtadi J, *et al.* Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access. 2018;6:19140-50.

38. Esposito C, De Santis A, Tortora G, Chang H, Choo K-KR. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing. 2018;5(1):31-7.

39. Huang Q, Yue W, He Y, Yang Y. Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. IEEE Access. 2018;6:36584-94.

40. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJ. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Transactions on Industrial Informatics. 2018;15(1):457-68.

41. Al-Shqeerat K, Al-Shrouf F, Hassan MR, Fajraoui H. Cloud computing security challenges in higher educational institutions-A survey. International Journal of Computer Applications. 2017;161(6):22-9.

42. Barona R, Anita EM, editors. A survey on data breach challenges in cloud computing security: Issues and threats. 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT); 2017: IEEE.

43. Bhushan K, Gupta BB. Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence. 2017;4(2):81-107.

44. Park J, Park J. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry. 2017;9:164.

45. Radwan T, Azer MA, Abdelbaki N. Cloud computing security: challenges and future trends. International Journal of Computer Applications in Technology. 2017;55(2):158-72.

46. Singh A, Chatterjee K. Cloud security issues and challenges. J Netw Comput Appl. 2017;79(C):88–115.

47. Mohit P, Amin R, Karati A, Biswas G, Khan MK. A standard mutual authentication protocol for cloud computing based health care system. Journal of medical systems. 2017;41(4):50.

48. Hussein NH, Khalid A. A survey of cloud computing security challenges and solutions. International Journal of Computer Science and Information Security. 2016;14(1):52.

49. Kaur M, Kaur K. A Comparative Review on Data Security Challenges in Cloud Computing. International Research Journal of Engineering and Technology. 2016;3(1).

50. Muthurajan V, Narayanasamy B. An Elliptic Curve Based Schnorr Cloud Security Model in Distributed Environment. TheScientificWorldJournal. 2016;2016:4913015.

51. Prakash C, Dasgupta S, editors. Cloud computing security analysis: Challenges and possible solutions. 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT); 2016: IEEE.

52. vurukonda N, Rao BT. A Study on Data Storage Security Issues in Cloud Computing. Procedia Computer Science. 2016;92:128-35.

53. Alasmari S, Anwar M, editors. Security & privacy challenges in IoT-based health cloud. 2016 International Conference on Computational Science and Computational Intelligence (CSCI); 2016: IEEE.

54. Albuquerque SL, Gondim PR. Security in cloud-computing-based mobile health. It Professional. 2016;18(3):37-44.

55. Casola V, Castiglione A, Choo K-KR, Esposito C. Healthcare-related data in the cloud: challenges and opportunities. IEEE cloud computing. 2016;3(6):10-4.

56. El Bouchti A, Bahsani S, Nahhal T, editors. Encryption as a service for data healthcare cloud security. 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT); 2016: IEEE.

57. Dorairaj SD, Kaliannan T. An adaptive multi-level security framework for the data stored in cloud environment. The Scientific World Journal. 2015;2015.

58. Kene SG, Theng DP, editors. A review on intrusion detection techniques for cloud computing and security challenges. 2015 2nd International Conference on Electronics and Communication Systems (ICECS); 2015: IEEE.

59. Liu Y, Sun YL, Ryoo J, Rizvi S, Vasilakos AV. A survey of security and privacy challenges in cloud computing: solutions and future directions. Journal of Computing Science and Engineering. 2015;9(3):119-33.

60. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information sciences. 2015;305:357-83.

61. Anand P, Ryoo J, Kim H, editors. Addressing Security Challenges in Cloud Computing—A Pattern-Based Approach. 2015 1st International Conference on Software Security and Assurance (ICSSA); 2015: IEEE.

62. Rao RV, Selvamani K. Data security challenges and its solutions in cloud computing. Procedia Computer Science. 2015;48:204-9.

63. Wang B, Zheng Y, Lou W, Hou YT. DDoS attack protection in the era of cloud computing and Software-Defined Networking. Computer Networks. 2015;81:308-19.

64. Wang Y, Tian Y, Tian L-L, Qian Y-M, Li J-S. An electronic medical record system with treatment recommendations based on patient similarity. Journal of medical systems. 2015;39(5):55.

65. Moosavi SR, Gia TN, Nigussie E, Rahmani A-M, Virtanen S, Tenhunen H, *et al.*, editors. Session resumption-based end-to-end security for healthcare internet-of-things. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; 2015: IEEE.

66. Zhang K, Yang K, Liang X, Su Z, Shen X, Luo HH. Security and privacy for mobile healthcare networks: from a quality of protection perspective. IEEE Wireless Communications. 2015;22(4):104-12.

67. Zhou J, Cao Z, Dong X, Lin X, editors. TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems. 2015 IEEE Conference on Computer Communications (INFOCOM); 2015: IEEE.

68. Khattak HAK, Abbass H, Naeem A, Saleem K, Iqbal W, editors. Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure. 2015 17th International Conference on E-health Networking, Application & Services (HealthCom); 2015: IEEE.

69. Mehraeen E, Ghazisaeedi M, Farzi J, Mirshekari S. Security Challenges in Healthcare Cloud Computing: A Systematic Review. Global Journal of Health Science. 2017;9(3):157-.

70. Sedik A, Hammad M, Abd El-Samie FE, Gupta BB, Abd El-Latif AA. Efficient deep learning approach for augmented detection of Coronavirus disease. Neural Computing and Applications. 2021.

71. Alsmirat MA, Al-Alem F, Al-Ayyoub M, Jararweh Y, Gupta B. Impact of digital fingerprint image quality on the fingerprint recognition accuracy. Multimedia Tools and Applications. 2019;78(3):3649-88.

72. Yu C, Li J, Li X, Ren X, Gupta BB. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools and Applications. 2018;77(4):4585-608.

73. Shweta K, Charu G. Ensure Hierarchal Identity Based Data Security in Cloud Environment. International Journal of Cloud Applications and Computing (IJCAC). 2019;9(4):21-36.

74. Al-Qerem A, Alauthman M, Almomani A, Gupta BB. IoT transaction processing through cooperative concurrency control on fog–cloud computing environment. Soft Computing. 2020;24(8):5695-711.

75. Scarfone K, Jansen W, Tracy M. Guide to general server security. NIST Special Publication. 2008;800(s 123).

76. Singh A, Chatterjee K. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. 2017;79:88-115.

77. Masud M, Gaba GS, Alqahtani S, Muhammad G, Gupta BB, Kumar P, *et al.* A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. IEEE Internet of Things Journal. 2020:1

78. Dorairaj SD, Kaliannan T. An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment. TheScientificWorldJournal. 2015;2015:601017.

79. Mehrtak M, Vatankhah S, Delgoshaei B, Gholipour A. Succession planning in the Iranian health system: A case study of the Ministry of Health and medical education. Global journal of health science. 2014 Sep;6(5):174.