World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(Research Article)

Security challenges and solutions using Cloud Computing

Firoz Mohammed Ozman *

Enterprise Architecture, Anecca Ideas Corp., Toronto, Ontario, Canada.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 738-750

Publication history: Received on 17 November 2024; revised on 26 December 2024; accepted on 28 December 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.2.0652

Abstract

Cloud computing is an excellent solution for today's digital challenges. Security is one of the significant problems in the technology, and the article's objectives are to identify security challenges and possible outcomes in cloud computing. A methodical assessment was conducted using PubMed, Scopus, and other databases. It has many benefits, such as fast deployments, mobility, flexibility, quality control, disaster recovery, and loss prevention. This article studies the usage and challenges of cloud computing in the healthcare industry. The data centralization within cloud systems poses severe security and privacy risks for healthcare providers and individuals. This is an appealing target for cyber attackers looking to steal sensitive information and intercept data as it travels while also shifting the ownership of that data to the cloud service providers. As a result, both parties lose their authority over sensitive data. Consequently, concerns regarding security, privacy, and efficiency limit the widespread implementation of cloud technology. Hence, there is a comprehensive requirement for a solution that equalizes all the conflicting requirements.

Keywords: Cloud computing; Internet; Healthcare services; Medicine

1. Introduction

In the healthcare sector, cloud computing refers to the use of remote servers accessed through the Internet to store, manage, and process health-related information. This approach contrasts with setting up an on-site data center with physical servers or keeping data on personal computers.

Cloud storage provides a versatile solution that enables healthcare providers and hospitals to utilize a network of remotely accessible servers, securely storing large amounts of data in an environment managed by IT experts. Following the implementation of the Electronic Medical Records Mandate, healthcare organizations throughout the United States have increasingly turned to cloud-based solutions to safeguard and manage patient records.

2. Clouding Computing

2.1. Cloud Definition

Individuals, research groups, and publications often define cloud computing in various ways. It refers to on-demand access to computing resources such as physical servers, data storage, virtual servers, network capabilities, application development tools, AI-driven analytical tools, software, and more via the Internet, with a pay-per-use pricing model.

2.2. Characteristics of Cloud Computing

The four key characteristics of Cloud computing

[*] Corresponding author: Firoz Mohammed Ozman.

- Shared resources: Users can concurrently access resources like networks, servers, applications, storage, memory, and processing capabilities. Service providers can adjust these resources in real time according to fluctuating demand, while users are entirely unaware of the physical locations of these services.
- On-demand self-service: Any user can manage scheduling, assess their storage and computing needs, and set **up** the cloud environment independently without needing assistance from service technicians.
- Network access: It enables extensive access to the network via the internet from any device
- Elasticity: It is adaptable and versatile, giving clients the impression that resources are boundless.

2.3. Cloud computing Service models

Models for cloud computing are divided into three categories:

Platform as a Service (PaaS) offers development and testing environments where consumers can create their applications on a virtual server. They have some control over the application hosting environment, especially regarding the application and data, which accelerates the development, testing, and deployment process.

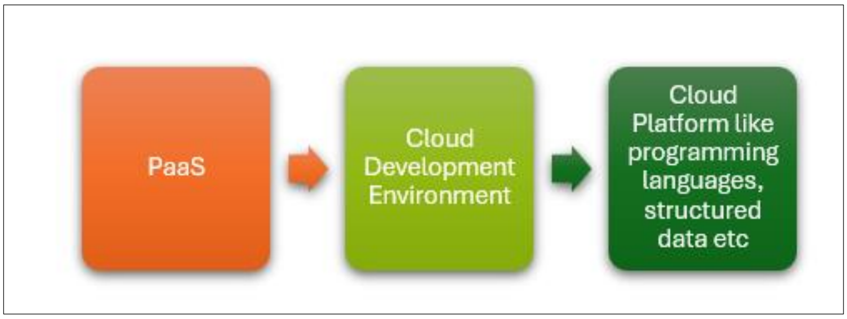
PaaS
Cloud Development Environment
Cloud Platform like programming languages, structured data etc

Figure 1 Flow Diagram for PaaS

Software as a Service (SaaS) is the most widely used cloud service. The software is hosted on the provider's platform. Consumers can access the software through a web browser or an application programming interface. This service operates on a pay-per-use business model. The main advantage is that consumers do not need to upgrade or maintain the software. There may be some limited options for application configuration available to them.

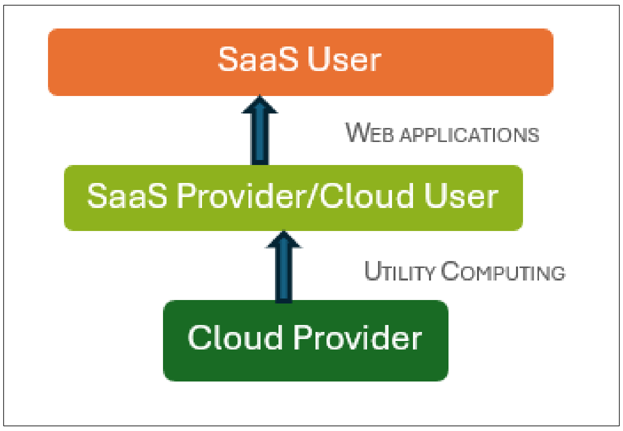

Figure 2 Flow Diagram for SaaS

Infrastructure as a Service (IaaS) supplies the infrastructure, operating systems, and applications. This is the most preferred service for companies needing more capital to purchase hardware. Customers are billed based on their usage. The infrastructure is scalable to meet varying storage requirements. Consumers have control over applications, middleware, operating systems, and data. However, consumers cannot control the underlying cloud infrastructure.

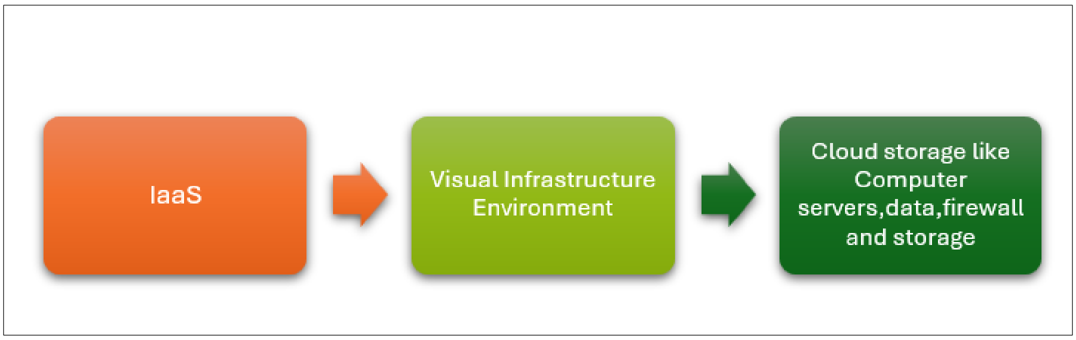
IaaS
Visual Infrastructure Environment
Cloud storage like Computer servers,data,firewall and storage

Figure 3 Flow Diagram for IaaS

2.4. Cloud Computing Delivery/Deployment models

2.4.1. Deployment models for cloud computing are divided into four categories

- Public cloud: The public cloud permits anyone to access systems and services. However, it may offer lower security since it is available to all. In this model, cloud infrastructure services are delivered over the Internet to the public or large industry sectors. The infrastructure in this cloud setup is owned by the service provider rather than the users.
- Private cloud: The private cloud deployment model fundamentally differs from the public cloud model. It provides a dedicated environment for a single user or customer, eliminating the need to share hardware with others. The key difference between private and public clouds lies in hardware management. Also, it allows access to systems and services within a specific organization or boundary.
- Hybrid cloud: A hybrid cloud integrates both public and private cloud settings, enabling organizations to leverage the advantages of each. It effectively handles traffic during high-demand times and offers enhanced flexibility, scalability, and cost efficiency compared to relying on just one cloud environment.
- Multi-cloud: Multi-cloud refers to the strategy of utilizing two or more cloud service providers simultaneously, which can include public, private, or a combination of both, to meet the objectives

3. Health Insurance Portability and Accountability Act (HIPAA)

Healthcare organizations manage large volumes of sensitive information, including patients' personal and medical data. HIPAA was established to safeguard patient privacy and security by outlining the guidelines and regulations that healthcare providers must adhere to when dealing with electronic protected health information (ePHI).

Cloud services that comply with HIPAA enable healthcare organizations to securely store, manage, and access electronic protected health information (ePHI) while adhering to regulations. These compliant services offer features like access controls, encryption, and auditing to guard the privacy, veracity, and accessibility of ePHI. This article will explore the most reliable cloud storage services that meet HIPAA compliance standards, on which healthcare providers can depend.

Healthcare professionals and IT leaders readily commend cloud computing for its scalability, cost-effectiveness, and adaptability while maintaining HIPAA compliance. Beyond these advantages, healthcare executives who must adhere to HIPAA regulations increasingly turn to the cloud for several reasons.

- Safe transmission of electronic information: With healthcare systems in the United States increasingly depending on cloud applications and telehealth services, managing patient data per HIPAA regulations is more straightforward in the cloud environment.
- Integrated business continuity options: IT professionals can focus less on physical security and disaster recovery when all data is stored on cloud services that comply with HIPAA regulations.
- Affordable entry point: Organizations gain from reduced initial expenses and savings on the purchase and upkeep of HIPAA-compliant hardware and infrastructure.
- Cost reductions: Many healthcare organizations experience savings on essential resources like physical space and staff time, as there’s no need for on-site server rooms or larger IT teams.
- Ongoing updates: Cloud hosting and storage allow centralized updates to be implemented and rolled out to users in a managed way from a testing environment.

3.1. HIPAA compliance for Cloud Storage is crucial.

As more organizations in the healthcare sector and their business partners transition their data to the cloud, ensuring HIPAA compliance for cloud storage has become crucial. Cloud storage enables healthcare providers to access medical records conveniently from any location. It also facilitates real-time collaboration among providers, which can enhance patient care.

However, achieving HIPAA compliance in cloud storage is a serious matter. A HIPAA-covered entity (CE) is any individual or organization managing patient information. HIPAA regulations apply to healthcare providers like doctors, hospitals, clinics, health plans, insurance companies, clearinghouses, and pharmacies. These entities must adhere to all HIPAA guidelines to safeguard protected health information (PHI).

3.2. The Risk to Data

Although cloud storage offers convenience and cost savings, it can pose risks to patient privacy if appropriate security measures are not in place. The HIPAA Security Rule requires covered entities and their business associates to implement physical, administrative, and mechanical protections to secure protected health information (PHI).

The safeguards outlined in the HIPAA Security Rule include encryption, access controls, and audit logs, but they are not inadequate. Furthermore, compliance with HIPAA also necessitates that covered entities and their business associates have a disaster recovery plan established to address potential data breaches or other emergencies.

3.3. Strategies for Protecting Protected Health Information

HIPAA-compliant data storage providers that deliver cloud computing services must adhere to the same standards. A covered entity and its business associate must accomplish equivalent physical, administrative, and technical safeguards to protect PHI and undergo regular audits to verify compliance with HIPAA regulations.

Additionally, HIPAA-compliant data storage providers must enter into a business associate agreement (BAA) with covered entities, specifying each party's responsibilities in safeguarding PHI. Finding a cloud storage provider with sufficiently strong security features that will agree to a business associate agreement can be challenging.

- Valuing Your Patients: Ensuring HIPAA-compliant cloud storage is a legal necessity and an ethical duty to patients. Individuals place their trust in healthcare organizations to handle their most sensitive information, and it is the responsibility of these organizations to safeguard that data. A data breach can severely undermine a patient's trust and lead to substantial financial penalties for the healthcare provider.

3.4. Enhanced Patient Outcomes

Beyond safeguarding patient privacy, HIPAA-compliant online storage can also enhance patient outcomes. When healthcare providers have easier access to patient information, they can deliver more accurate diagnoses and develop better treatment plans. Additionally, real-time collaboration among healthcare professionals can further improve patient care and lead to more favourable outcomes. AWS, Microsoft Azure, Google Cloud, Box, Dropbox Business, Sync, and Egnyte are the leading HIPAA-compliant cloud Storage Solutions.

3.5. Business Associate Agreement (BAA)

Business Associate Agreements (BAA) are legal contracts between two parties, typically involving a covered entity (CE) and a business associate (BA). This agreement outlines that the BA will provide services for the CE related to electronic protected health information (ePHI) and is responsible for ensuring that all activities conducted on behalf of the CE comply with HIPAA regulations and the terms specified in the agreement.

The BAA also specifies the duties and responsibilities the BA must fulfill, including maintaining security and privacy measures, training employees on HIPAA guidelines, responding to requests from CEs, promptly reporting any breaches or violations, and implementing corrective actions. By entering a BAA with an entity that handles PHI, businesses are legally required to safeguard their clients' data per HIPAA standards.

4. Design and Methods

4.1. Design

The systematic review aimed to enhance the consideration gained from prior studies by gathering pertinent published articles. An extensive literature quest was conducted using Science Direct, PubMed, Scopus, and Web of Science Online databases. Two investigators collaborated to execute the quest and identify relevant publications online.

The studies were primarily included based on the inclusion criteria, utilizing specific keywords in the abstract. Articles that were not related to the current research or did not have inventive information were eliminated. The secondary stage also involves a detailed, complete manuscript assessment of the selected articles to determine the most suitable ones for inclusion.

This study seeks to tackle the following concerns within contemporary healthcare systems:

- The primary challenge is jeopardizing the security of cloud computing.
- The strategies can be implemented to mitigate these potential issues.

We selected studies aligned with our research goals, covering the period from early 2016 to December 2019. The criteria of exclusion include:

- Primary findings are commencing from unfinished projects.
- The works lack full-text manuscripts, abstracts, and discussion presentations.
- Publications that do not provide original findings, Journal articles
- Articles that do not offer free access to the full text.

4.2. Research method

This article's objectives are to highlight study inclinations and pinpoint upcoming study directions related to the digital revolution in the field of Healthcare. To accomplish this objective, the study utilized a systematic literature review (SLR), which has proven to be an effective technique for uncovering study inclinations and outlining upcoming study possibilities. This article adhered to a structured method for recognizing and analyzing study articles according to SLR protocols. In this context, we followed the guidelines established in earlier studies on conducting systematic literature reviews. The entire literature review process is detailed in Figure 4

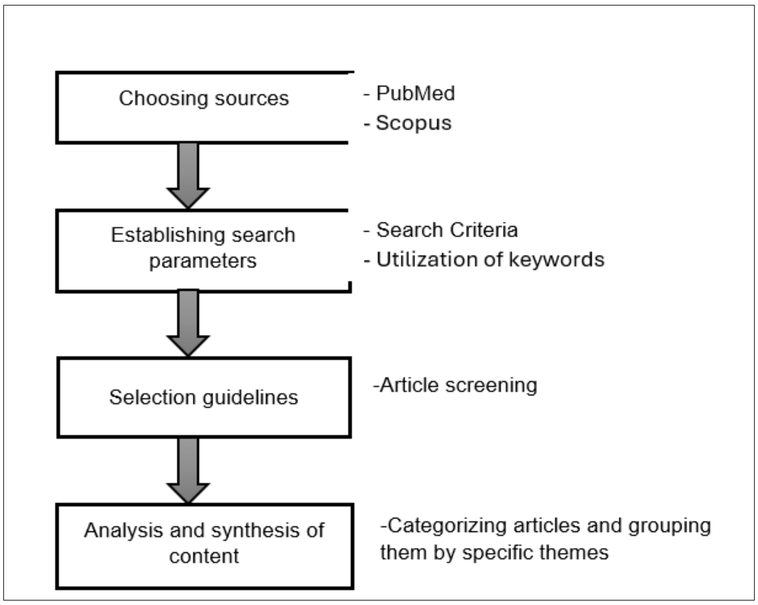
Choosing sources
- PubMed
- Scopus
Establishing search parameters
- Search Criteria
- Utilization of keywords
Selection guidelines
-Article screening
Analysis and synthesis of content
-Categorizing articles and grouping them by specific themes

Figure 4 Overview of the literature review process

4.3. Choosing sources

Considering the interdisciplinary focus of this research on digital transformation, such as cloud computing in health care, we utilized several databases to ensure comprehensive article exposure. An available quest was performed across Scopus, ScienceDirect, and Web of Science. We depended primarily on Scopus and ScienceDirect for access to relevant articles due to their availability of full texts. Scopus offers extensive coverage in social sciences and various interdisciplinary areas, while ScienceDirect facilitates broad searches across entire arenas and provides progressive quest options tailored to definite topics.

4.4. Establishing search parameters

The search was carried out in two stages. We concentrated on finding existing inclinations in the healthcare sector in the initial stage. In the subsequent stage, we broadened our search to include digital technologies facilitating transformations. Our focus was on the digital technologies outlined in the framework, encompassing social media, mobile technology, analytics, cloud computing, the Internet of Things, and artificial intelligence. These technologies are recognized as catalysts for digital transformation across organizations.

Employing suitable keywords is crucial for locating high-quality research articles. Given the transient nature of IT literature keywords, selecting keywords should be viewed as a dynamic step that requires an ongoing approach. To maximize the comprehensiveness of our search, we adhered to specific strategies and guidelines for keyword selection and literature exploration. Following the recommendations for keyword selection, we utilized both backward and forward search methods to enhance the quality of our literature search results.

We employed reference search techniques to retain the relevant papers identified through these keywords. By examining the bibliography sections of these papers, we gained more profound insights into the literature trends within our research domain. However, as previously noted, our primary focus was on the impact of digital technologies such as cloud computing on health care. Consequently, we distinguished our keywords during the second stage of our quest.

4.5. Selection guidelines

The extensive search of existing literature yielded many articles; however, we concentrated solely on those pertinent to our study inquiry, guided by the earlier criteria. These include: The article must address health care and incorporate any of the specified digital technologies. The study should demonstrate real applications for mitigating healthcare effects.

The article must be an available investigational study in an international journal paper that was accepted if it is available in the Scopus database.

This was a clear criterion for selecting articles for the final review. Each article was thoroughly examined, and a sample was chosen for further analysis. During the initial screening phase, we created a table that captured essential publication details, such as the paper's title, author, publication year, and journal name. Each article was summarized individually in the table to ensure a comprehensive sample understanding.

4.6. Analysis and synthesis of content

Once we finalized our sample of articles, we carried out an in-depth content analysis. Similar to our literature quest, we employed a systematic approach to analyze the selected articles. We created a comprehensive table to classify each article based on scope, area of focus, and technology emphasis. The chosen articles highlighted the application of various digital technologies to mitigate the effects by enhancing different organizational functions and processes. We examined them closely and drew significant conclusions from our analysis. The key findings are mentioned below.

5. Results

Using the specified search strategy, we identified 1021 full texts of relevant studies. After a thorough review, we found and removed 430 duplicates. Next, two individual reviewers assessed the titles and abstracts of the remaining (591 resources). We then reviewed the full texts of the selected articles, ultimately identifying (226 resources) that were most relevant according to our eligibility criteria. Based on these criteria, we excluded 143 articles, which comprised (n=28) review articles, (n=19) opinion articles, and (n=133) unrelated to cloud security. Ultimately, 83 studies experienced the inclusion criteria and were incorporated into the final assessment.

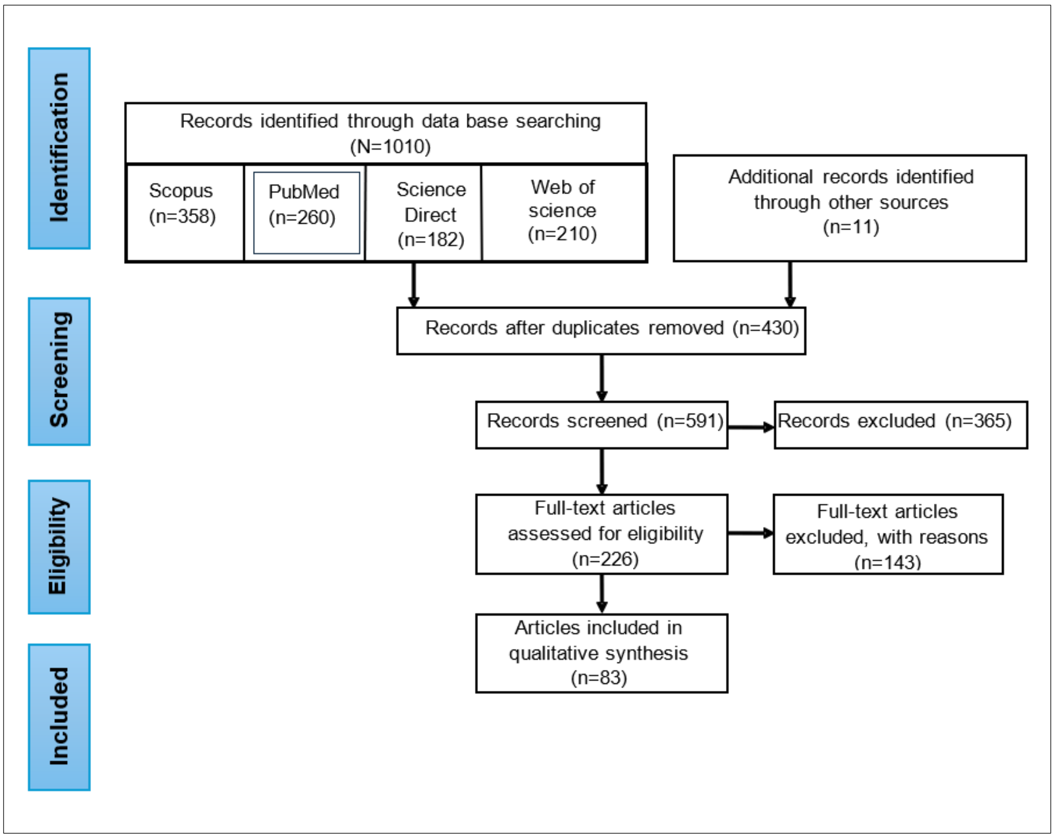
Identification
Screening
Eligibility
Included
Records identified through data base searching (N=1010)
Scopus (n=358)
PubMed (n=260)
Science Direct (n=182)
Web of science (n=210)
Additional records identified through other sources (n=11)
Records after duplicates removed (n=430)
Records screened (n=591)
Records excluded (n=365)
Full-text articles assessed for eligibility (n=226)
Full-text articles excluded, with reasons (n=143)
Articles included in qualitative synthesis (n=83)

Figure 5 The process for identifying the target articles was conducted in accordance with the PRISMA standards.

As per the studies, the prevalent security challenges and solutions in cloud computing are found, and the research is outlined in Table 1. The common challenges were confidentiality (n=18), data breach (n=15), and network security (n=12). The data with frequency is shown below in Figure 6. Also, Authentication (n=16), data classification (n=9), access control (n=8), and black chain (n=5) were the best familiar results for the security challenges in cloud base Figure 7.

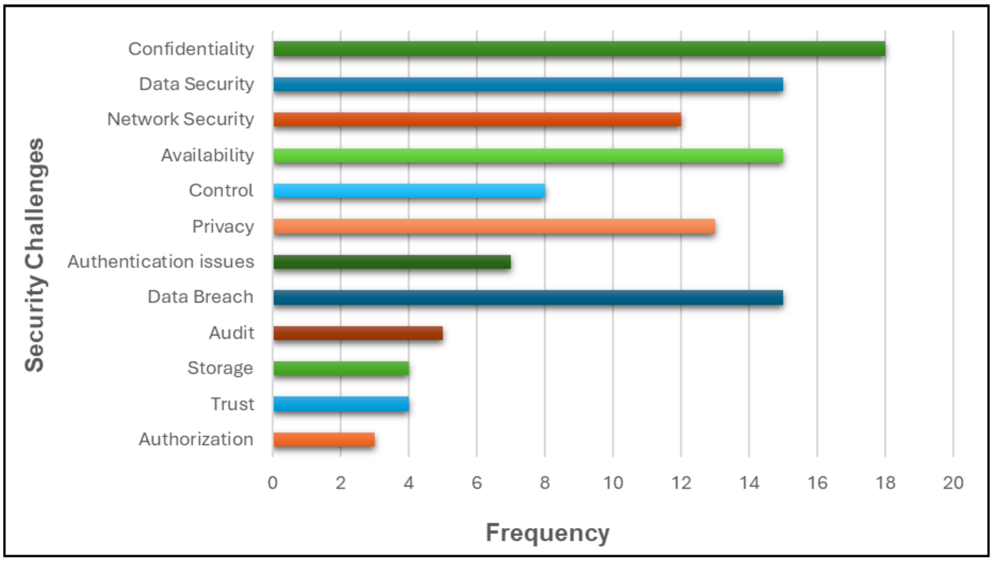

Figure 6 The frequency of security issues in cloud computing

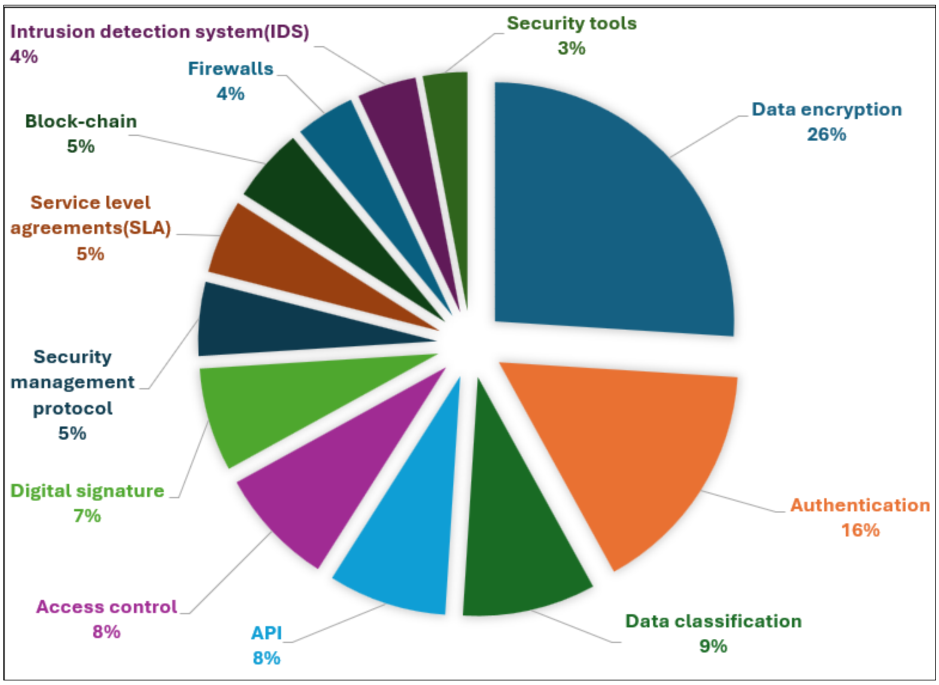

Figure 7 The most frequently recognized solutions for tackling security challenges in cloud computing

Table 1 Recognized Security Issues and Possible Remedies in Cloud Computing for Healthcare

S. No.	Title	Release Year	Security Issues	Recommended Approaches	New Author
1	A survey on security challenges in cloud computing: issues, threats, and solutions	2020	Protective measures for data. User-focused security measures, Information storage solutions. Network safeguards.	Information encoding (encryption techniques, quantum encryption), Hash algorithms, message verification, authentication Codes; Systems for detecting and preventing unauthorized access, Security barriers, packet screening, electronic signatures, certification, notarization, public and private distributed ledgers.	Rafsanjani MK
2	A biometric authentication and data management system for healthcare data in cloud	2020	Enhancing the functionalities of health apps on mobile platforms like tablets laptops and smartphones unauthorized use of personal information fraudulent tax activities healthcare deception financial institution fraud insurance scams slander against prominent patient.	Authentication systems based on biometric data BAMHealthCloud safeguards electronic medical information access through behavioral analysis; signature sample training for verification has been conducted simultaneously on the Hadoop MapReduce framework utilizing resilient backpropagation neural networks, ALGO Health Security conducts security assessment	Zareen FJ

				using a parallelized MapReduce programming approach.	
3	Cloud Computing and Data Security Challenges	2019	Information retrieval and privacy challenges	Data protection and encryption	Shakya S
4	Securing Healthcare Information over cloud using hybrid approach	2019	Protecting data is a crucial element that limits the adoption of cloud systems.	Implementing network coding along with re-encryption utilizing EIGamal encryption in a hybrid model to safeguard healthcare data in the cloud	Kapadia N
5	Cloud computing security challenges & solutions	2018	Privacy, reliability, accessibility	--	Bardhan A
6	Recent security challenges in cloud computing	2018	Risks and vulnerabilities in cloud computing, security in encrypted cloud environments	IaaS, PaaS, SaaS	Jeyaraj A
7	Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing	2018	Risks and vulnerabilities in cloud computing, security in encrypted cloud environments	Encryption	Yue W, He Y
8	Cloud computing challenges in higher education institutions	2017	Network protection, user access management, cloud architecture, information security	Ensuring that the administrator can oversee and manage cloud resources and services when finalizing contracts with service providers, establishing an agreement with a third party to continue regular audits to access the performance and compliance of the service provider with the agreed upon terms billiard periodically evaluating the performance of available cloud service and resources. Classifying data and applications in the cloud environment according to their significance and sensitivity not all information stored in the cloud is considered highly secure implementing backup and recovery solutions. Utilizing appropriate authentication authorization and access security tools and strategies. Offering robust encryption protocol and key management for data at rest, in transit and doing backup.	Al-Shrouf F
9	Security challenges in cloud computing	2017	Concerns at physical security level, software and application security challenges, network	Categorization based on technique employed, classification according to attack detection method,	Gupta BB

			security vulnerabilities, data protection issues, computational challenges, management and account oversight issues, trust related challenges, regulatory and legal compliance matters.	classification by response time, classification based on the point of deployment, classification by the extent of deployment, classification by the level of collaboration, classification based on defensive actions, classifications by response strategy.	
10	Cloud computing security challenges and future trends	2017	Authorized access, information storage, accessibility, support for investigation, adherence to regulations, data separation, restoration, sustainability	Validation, approval	Azer MA
11	A standard mutual authentication protocol for cloud computing based healthcare system	2017	Safeguarding is crucial for patient medical records due to the highly sensitive nature of the information. It's important to maintain patient confidentiality	Validation procedure using cloud technology	Amin R
12	Cloud computing security analysis challenges and possible solutions	2016	Challenges related to deployment models, service models, and network concerns	Resource isolation through segmentation. Creation of a dedicated application. Implementation of robust 2 factor authentication	Dasgupta S
13	An adaptive multi-level security framework for the data stored in cloud environment	2015	Privacy	User access management, verification of data integrity, data categorization	Kaliannan T
14	A survey of security and privacy challenges in cloud computing solutions and future directions	2015	Insufficient transparency shared tenancy	Data protection	Sun YL
15	Addressing security challenges in cloud computing a pattern-based approach.	2015	Traffic in. Interception, Information leaks., data loss., vulnerable APIs., service disruption attacks., misuse of clouds resources., insider threats.	--	Ryoo J
16	A session resumption-based end to end security for healthcare. Internet of Things.	2015.	Comprehensive security for healthcare IoT.	A session continuation-based Security model for healthcare IoT.	Gia TN
17	TR-MABE: white box traceable and revocable multi authority attribute-based encryption and its application to	2015.	Cloud security for eHealthcare.	Perceptible. Multi-expert trait-built encoding design to efficiently maintain multi-level privacy without the need for additional unique signatures. Utilizing secret key to safeguard	Cao Z

	multi-level privacy preserving E health cloud computing systems.			patient Identities and protected health information.	

6. Discussion

Cloud computing is an innovative technology that ensures the accessibility of patient data everywhere. However, it faces significant hurdles in addressing one of the healthcare sector's most pressing needs. Due to its fundamental characteristics, like inaccessible information storage and the absence of a precise network environment, implementing robust security measures is crucial. Consequently, effectively recognizing security tasks and developing suitable keys is vital for service providers and the companies that utilize this technology.

AI has demonstrated a promising potential in addressing health challenges, particularly when integrated with cloud computing. A deep learning AI tool designed to rapidly screen corona patients was developed using chest X-rays. This approach was implemented via a cloud process wherever a radiography kit was available.

The current study highlights that the primary challenge in this skill is ensuring data security. Mean individuals can compromise data security. Various resolutions are available to safeguard data, with data encryption being the most crucial. Encryption is a fundamental layer of defence within cybersecurity frameworks, making unauthorized access to data as challenging as possible. Encryption techniques are designed to create schemes that can only be breached with substantial computational power. Data encryption was identified as an effective method for protecting data from security risks. Also, the findings of this research advance reinforce data encryption as the most effective result for ensuring data security.

The current research findings indicate that confidentiality ranks as the second most significant challenge in cloud technology. This concept involves safeguarding data from unauthorized access and confirming that delicate data is only accessible with proper approval. The management of cloud data can heighten the risk of data breaches. For the patient-doctor relationship to function effectively, patients must trust that the healthcare system will protect their data privacy. Research has demonstrated that confidentiality can be maintained through access control and authentication measures. A Common Endorsement and Secret Key formation protocol has been introduced during the Internet of Medical Things realm for Corona patients. As a result, it effectively tackles issues related to privacy, validation, and integrity, thereby protecting the subtle health data of patients.

This study indicates that veracity, accessibility, and network security are critical concerns within cloud computing infrastructure. The developmental research faces many significant challenges in deploying cloud-based services, particularly since the loss or exposure of information can lead to substantial legal or business repercussions. Confidentiality, integrity, and availability are recognized as the three primary components of cloud system protection, and they are considered for assessment in this context.

As a result, ensuring network security within cloud setup has become a significant concern for companies. Widespread network outbreaks typically occur at the network layer, counting threats like Internet protocol tracking and interface probing attacks. Attackers, for example, can flood cloud computing environments with a large volume of requests to gain access to virtual machines, thereby limiting their availability to legitimate users; this is known as a Denial of Service (DoS) attack. This type of outbreak explicitly targets the availability of cloud resources. Related studies indicate that there is no established security specification for implementing security restrictions in wireless networks. Nevertheless, probable solutions such as APIs, data division, and security management protocols can be utilized to maintain security within cloud systems.

7. Conclusion

Cloud computing provides numerous advantages regarding data access and space, especially for healthcare establishments, in addition to related research. While cloud computing conditions are viewed as a promising Cyberspace-built platform, significant protection issues exist. This unease arises from the cloud computing model's shared, virtualized, and public characteristics. To facilitate the adoption of cloud computing, it is essential to address these challenges by creating innovative solutions. All users, whether persons or companies, must remain adequately aware of the security risks associated with this technology.

This research provides a comprehensive summary of cloud computing and a review of the security challenges and solutions that have emerged over the past five years. This technology uses encryption to store and retrieve information to ensure secure data access. We have furthermore examined several key issues that complicate cloud security engineering. Recognizing these issues is the initial stage toward addressing them, and upcoming research should focus on developing more practical solutions to resolve these issues.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest is to be disclosed.

References

[1] Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; PRISMA, G. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. PLoS Med. 2009, 6, e1000097. [Google Scholar] [CrossRef] [PubMed] [Green Version]

[2] Levy, Y.; Ellis, T.J. A systems approach to conduct an effective literature review supporting information systems research. Inf. Sci. 2006, 9, 181–212. [Google Scholar] [CrossRef] [Green Version]

[3] Payne, T. H., Bates, D. W., Berner, E. S., Bernstam, E. V., Covvey, H. D., Frisse, M. E., Graf, T., Greenes, R. A., Hoffer, E. P., and Kuperman, G., Healthcare information technology and economics. Journal of the American Medical Informatics Association 20(2):212–217, 2013.

[4] Agarwal, R.; Gao, G.D.; DesRoches, C.; Jha, A.K. The Digital Transformation of Healthcare: Current Status and the Road Ahead. Inform. Syst. Res. 2010, 21, 796–809. [Google Scholar] [CrossRef] [Green Version]

[5] Hussain, S. An efficient and economical multi-cloud storage in cloud computing. IET 2012, 185–191. [Google Scholar] [CrossRef]

[6] Rashid, F.; Miri, A.; Woungang, I. Secure enterprise data deduplication in the cloud. In Proceedings of the IEEE International Conference on Cloud Computing (CLOUD), Santa Clara, CA, USA, 28 June–3 July 2013; pp. 367–374. [Google Scholar]

[7] Melo, M.; Maciel, P.; Araujo, J.; Matos, R.; Araujo, C. Availability study on cloud computing environments: Live migration as a rejuvenation mechanism. In Proceedings of the International Conference on Dependable Systems and Networks, Budapest, Hungary, 24–27 June 2013; pp. 1–6. [Google Scholar] [CrossRef]

[8] Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H. A survey on the Internet of Things and cloud computing for healthcare. Electronics 2019, 8, 768. [Google Scholar] [CrossRef] [Green Version]

[9] Buyya R., Yeo C. S., Venugopal S., Broberg J., and Brandic I., Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems. (2009) 25, no. 6, 599–616, 2-s2.0-63649117166, https://doi.org/10.1016/j.future.2008.12.001.

[10] Goldzweig, C. L., Towfigh, A., Maglione, M., and Shekelle, P. G., Costs and benefits of health information technology: new trends from the literature. Health Affairs 28(2):w282–w293, 2009.

[11] Preethi M, Balakrishnan R, editors. Cloud-enabled patient-centric EHR management system. IEEE Conference of Advanced Communication Control and Computing Technologies (ACCT); 2014. pp. 1678–80. [Google Scholar]

[12] Li, M.; Yu, S.; Ren, K.; Lou, W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010), Singapore, 7–9 September 2010; pp. 89–106. [Google Scholar]

[13] Zhang, Q.; Wang, X.; Yuan, J.; Liu, L.; Wang, R.; Huang, H.; Li, Y. A hierarchical group key agreement protocol using orientable attributes for cloud computing. Inform. Sci. 2019, 480, 55–69. [Google Scholar] [CrossRef]

[14] Dong, X., Yu, J., Luo, Y., Chen, Y., Xue, G., and Li, M., Achieving a practical, scalable and privacy-preserving data sharing service in cloud computing. Comput. Sec. 42:151–164, 2014. doi:10.1016/j.cose.2013.12.002.

[15] Wooten, R., Klink, R., Sinek, F., Bai, Y., and Sharma, M., Design and implementation of a secure healthcare social cloud system. 2012 12Th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (Ccgrid 2012). 805–810, 2012. doi:10.1109/CCGrid.2012.131.

[16] Yang, J., Li, J., and Niu, Y., A hybrid solution for privacy-preserving medical data sharing in the cloud environment. Futur. Gener. Comput. Syst. 43–44:74–86, 2015. doi:10.1016/j.future.2014.06.004.

[17] Zhou, J., Cao, Z., Dong, X., Xiong, N., and Vasilakos, A., 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf. Sci. 314:255–276, 2015. doi:10.1016/j.ins.2014.09.003.

[18] Wang, C., Zhang, B., Ren, K., M. Roveda, J., Wen Chen, C., and Xu, Z., A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing. IEEE INFOCOM 2014 - IEEE Conf. Comput. Communi. 2130–2138, 2014. doi:10.1109/INFOCOM.2014.6848155.

[19] Barua, M., Liang, X., Lu, R., and Shen, X., ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing. Int. J. Sec. Networks 6(2/3):67–76, 2011. doi:10.1504/ijsn.2011.043666.

[20] Löhr, H., Sadeghi, A., and Winandy, M., Securing the e-health cloud. Proc. ACM Int. Conf. Health Inform. - IHI ’10. 220–229, 2010. doi: 10.1145/1882992.1883024.

[21] Chen, C., Yang, T., Chiang, M., and Shih, T., A privacy authentication scheme based on cloud for medical environment. J. Med. Syst. 38:143, 2014. doi:10.1007/s10916-014-0143-9.

[22] Benaloh J, Chase M, Horvitz E, Lauter K (2009) Patient controlled encryption: ensuring privacy of electronic medical records. In: CCSW ’09 proceedings of the 2009 ACM workshop on cloud computing security, pp 103–114.

[23] Li J, Huang X, Li J, Chen X, Xiang Y (2013) Securely Outsourcing Attribute-based Encryption with Checkability. IEEE Trans Parallel Distrib Syst. doi:10.1109/TPDS.2013.271.