IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Securing Member Data In Health Cloud Environments

Sourabh Mahajan
Himani Gupta

Abstract

The proliferation of cloud computing in the medical field has altered the method of storing, managing and sharing of medical information and has made it more accessible and collaborative by the various stakeholders. Nevertheless, this change also creates serious problems with the security and privacy of sensitive member information stored on health clouds. Such threats like unauthorized access, data breach, and insider abuse pose a constant challenge to the trust and the adherence to the regulatory standards. To overcome these threats, scientists have suggested a plethora of solutions such as encryption-based systems, attribute- and role-based access control systems, blockchain-based solutions to secure data sharing, and extensions to fog computers to improve privacy and reduce latency. Latest literature presents the significance of incorporating the concept of multi-layered security models that integrate cryptographic methods with decentralized trust to protect member data and guarantee the ability to scale the system and interoperability. Although significant progress is being made, there are still gaps in the security of real time data exchange, cross platform interoperability and security versus performance. This paper reviews the current methods, analyzes the emerging technologies, and outlines the future plans to have robust, privacy-centered, and efficient health cloud security systems.

Keywords: Health cloud; Data security; Privacy preservation; Secure data sharing; Access control; Blockchain; Electronic Health Records (EHRs).

I. Introduction

Due to the quick digitization of healthcare, cloud computing has been widely used to store, manage, and share sensitive medical data. The health cloud environments are scalable, cost-effective, and have ubiquitous access to patient records, which makes them appealing substitutes to the traditional storage systems. These platforms allow healthcare providers, insurance companies and patient to work in harmony and at the same time maintain the flow of service delivery. Nevertheless, the use of cloud infrastructures has severe implications on the confidentiality, integrity, and availability of member data, which in many cases contains extremely sensitive health information that is subject to cybercrimes and abuse (Zhang and Liu, 2010; Abbas and Khan, 2014).

Maintaining the security and privacy of data without compromise of the efficiency of the cloud-based healthcare system and their interoperability is the central issue. Traditional frameworks of central data management are not always enough, and healthcare cloud solutions are prone to insider attacks, unauthorized access, and data breach that can lead to massive financial and reputational losses (Al-Issa, Ottom, and Tamrawi, 2019; Abrar et al., 2018). To overcome these difficulties, scientists have suggested a variety of solutions including cryptographic tools, access control systems, blockchain, and fog computing systems. As an example, attribute-based encryption and fine-grained access control have been implemented to protect personal health records (Li, Yu, Zheng, Ren, and Lou, 2012; Li, Yu, Ren, and Lou, 2010), and blockchain-based models provide additional security measures in the form of tamper-proof disclosure and decentralized confidence in transactions with health data (Nguyen, Pathirana, Ding, and Seneviratne, 2019; Xia, Sifah, Smahi, Amofa, and

Furthermore, multi-level security that combines layers of security is also becoming an attractive proposal to strike the right balance of performance and protection. Research has also emphasized the need to combine encryption, patient-centred access control, and decentralized models to enhance the security of healthcare information (Yang, Li, and Niu, 2015; Ali et al., 2018). Recent literature reviews also mention that it is necessary to develop comprehensive frameworks

that should not only be technical but also comply with regulatory documents including HIPAA and GDPR that introduce rigorous data protection guidelines (Kotha et al., 2022; Sahi, Lai, and Li, 2021).

In spite of all these developments, there exist major gaps in research. The challenges to achieve interoperability in various healthcare eco-systems, scalability across multi-cloud systems and real-time secure data exchange remain a challenge (Fabian, Ermakova, and Junghanns, 2015; Thilakanathan et al., 2014). Moreover, new technologies like Healthcare 4.0, cyber-physical systems, and modular encryption standards are changing the future of health cloud security, and new solutions must be developed to guarantee the sustainable protection of member data (Qiu, Qiu, Liu, and Memmi, 2020; Shabbir et al., 2021).

Thus, this paper analyses the current best practices in securing member data in health cloud environments. It examines the current security measures, highlights the critical areas of concern and examines the future trends in achieving effective, privacy-aware and powerful health clouds. Through the theoretical examination of encryption models, access control methods, applications of blockchain, and extensions of fog computing, the work will engage in the current discussion of securing sensitive healthcare data in digital environments.

The increase in the use of health cloud environments underlines the necessity to find a balance between usability and powerful data protection tools. Healthcare organizations are being pressed continuously to embrace cloud solutions that enable them to share data, perform analytics, and achieve interoperability in addition to maintaining severe privacy regulations and ethical liabilities. Insecure storage and transmission of health records are, not only technically, but also socially and legally risky, because patients want their records to be confidential and trusted by the systems that deal with their sensitive medical histories (Esposito, De Santis, Tortora, Chang, and Choo, 2018; Hwang and Li, 2010). The inability to secure these systems can affect the confidence in transformation in digital healthcare hindering innovation and usage of cloud-based technologies.

Aim of the Study

The main purpose of the study is to investigate and analyze previous and new mechanisms to secure the member data in the health cloud environment. It aims at giving a detailed analysis of the technologies, frameworks, and models that have the potential to guarantee confidentiality, integrity, and availability of healthcare data and facilitating efficient and scalable service delivery.

Objectives of the Study

In this respect the study is directed by the following objectives:

i. To analyze the current information security issues in health clouds, such as access control concerns, data breach, and compliance with regulation (Al Hamid, Rahman, Hossain, Almogren, and Alamri, 2017; Abrar et al., 2018).
ii. In order to examine encryption and cryptography methods, which are applied to protect personal health records, and provide control over the access to data at the fine-grain level (Li et al., 2012; Shabbir et al., 2021).
iii. In order to assess access control models, such as patient-centric, role-based, and trust-based models, which are developed to support multi-user and multi-owner health cloud settings (Butt et al., 2023; Ali et al., 2015).
iv. To investigate the blockchain and distributed ledgers in decentralized, transparent and tamper-resistant information sharing in e-health ecosystems (Xia et al., 2017; Nguyen et al., 2019).
v. To determine the newly emerging trends and technologies, e.g. fog computing, Healthcare 4.0, and modular encryption standards that can further improve security and privacy in health cloud environments (Qiu et al., 2020; Kotha et al., 2022).

These aims and objectives put this paper in a position of being a complete overview of the current situation in health cloud security as well as being a prospective analysis of future trends. This two-fold consideration makes sure that the discussion will be influencing both scholarly conversation and real-life applications to the healthcare organizations and policy-making. Finally, the study highlights the significance of establishing trustful, resilient and compliant cloud systems capable of securing the data of members and enabling transformation of healthcare digitally.

II. LITERATURE REVIEW

a. History of Health Cloud Security.

The introduction of cloud computing in health care has revolutionized data storage and sharing, and offers a solution that is scalable and cost effective. Nevertheless, initial studies found underlying security vulnerabilities, especially in terms of access control, data confidentiality and trust management (Zhang and Liu, 2010). Abbas and Khan (2014) also pointed out that to safeguard health information in e-health clouds, privacy-preserving models, which can deal with both internal and external threats, are needed. These initial studies formed the basis of the creation of superior security systems, with the patient-centric models being in urgent need.

b. Privacy and Security Models

There are numerous models that are advanced by researchers to protect sensitive medical data. ABE schemes, such as attribute-based encryption, can be used to enable fine-grained access control to personal health records, enabling patients to grant access control (Li, Yu, Zheng, Ren, and Lou, 2012). In a similar manner, trust-based models of role-based access control (RBAC) have been extended to allow optimisation of decision-making in multi-user contexts (Butt et al., 2023). Hybrid methods involving a combination of encryption and policy-based controls have also been considered and balance the usability and security (Yang, Li, and Niu, 2015).

c. Data Sharing methods using security strategies.

Data sharing is a key issue in health clouds that is best ensured by security. Fabian, Ermakova, and Junghanns (2015) proposed collaborative multi-cloud systems designs, and Thilakanathan et al. (2014) created secure health monitoring and sharing platforms. The solution has become a ground-breaking one because blockchain technology enables immutable, transparent and decentralized data management. Medical data sharing across providers without trust can be made possible by the MeDShare (Xia, Sifah, Asamoah, Gao, Du, and Guizani, 2017) or BBDS (Xia, Sifah, Smahi, Amofa, and Zhang, 2017) models. Equally, Nguyen, Pathirana, Ding, and Seneviratne (2019) indicated that blockchain would be useful in the management of secure EHR sharing in mobile cloud computing.

d. In-depth Reviews and State of Art Surveys.

There are a number of review papers that have synthesized security challenges and opportunities. Kotha et al. (2022) systematically analyzed the information on secure data sharing in clouds, and Jin, Luo, Li, and Mathew (2019) offered the information on the frameworks of privacy preservation in medical data sharing. A state-of-the-art review by Sahi, Lai, and Li (2021) claims that there are still significant gaps in compliance and interoperability and that frameworks have to be flexible. These papers affirm that despite the achieved progress, such aspects as scalability, regulatory compliance, and protection in real-time are under-researched.

e. Emerging Trends in Health Cloud Security

The technology behind health clouds is undergoing change, and this paper will examine future trends in cloud security.

Computer improvements have led to the emergence of Healthcare 4.0 and cyber-physical systems that depend on secure sharing of data to provide precision medicine and remote monitoring. Qiu, Qiu, Liu, and Memmi (2020) suggested secure data sharing models to be used by cyber-physical systems in healthcare. Next-generation implements have also been proposed, specifically modular encryption standards on mobile health systems (Shabbir et al., 2021) and fog computing-based security models (Al Hamid, Rahman, Hossain, Almogren, and Alamri, 2017). It is estimated that blockchain along with artificial intelligence will increase privacy and efficiency in handling big data in the healthcare sector (Esposito, De Santis, Tortora, Chang, and Choo, 2018).

f. Goals and Objective of Literature Analysis.

The intention behind the review of the previous literature is to synthesize the results of the existing health cloud security solutions and determine areas where they are inapplicable. In particular, they are aimed at accomplishing:

i. Evaluate the level of protection of the information of members through the current encryption and access control procedures.
ii. Compare the solutions based on blockchain with the traditional approaches to the integrity and trust of data.
iii. Consider the potential of new technologies, including Healthcare 4.0 and fog computing, to help solve the current issues.
iv. Point out restrictions and suggest areas of future investigation.

g. Case: Blockchain in Secure Sharing of Medical Data.

An appropriate case study that depicts how health cloud security can be applied in practice is the use of electronic medical records (EMRs) systems that utilise blockchain technology. Xia, Sifah, Asamoah, Gao, Du, and Guizani (2017) suggested MeDShare, which is a blockchain system that allows the sharing of EMRs among cloud providers without trust. Their system guaranteed that unauthorized changes are not allowed and also was able to scale and be transparent. Equally, Nguyen et al. (2019) provided a test on blockchain in mobile cloud-based e-health systems and established that blockchain is capable of supporting real-time EHR exchanges over distributed networks. These case studies reveal the feasibility of blockchain to solve old problems of trust, integrity and compliance in health clouds.

Table 1: Comparative Summary.

Approach	Key Mechanism	Strengths	Limitations	References
Attribute-Based Encryption (ABE)	Cryptographic fine-grained access control	Patient-centric, scalable	High computational cost	Li et al. (2012); Li et al. (2010)
Role-Based Access Control (RBAC)	Role and trust-based authorization	Simple, efficient	Limited flexibility in dynamic settings	Butt et al. (2023); Ali et al. (2015)
Blockchain Models (MeDShare, BBDS, SeSPHR)	Decentralized ledger for secure sharing	Transparency, immutability	Scalability, energy cost	Xia et al. (2017); Nguyen et al. (2019); Ali et al. (2018)
Fog Computing Security	Decentralized processing close to data source	Reduced latency, improved privacy	Complexity in deployment	Al Hamid et al. (2017)
Hybrid Models	Combination of cryptography + access control	Balanced efficiency and security	Still experimental	Yang et al. (2015); Qiu et al. (2020)

h. issues in Health Cloud Systems.

Even though technological innovations increase the possibility of securing the health cloud systems, a number of challenges have persisted. Data privacy has been a priority because the sensitive information of members is becoming more vulnerable to unauthorized access because of security vulnerabilities in multi-cloud setups (Fabian, Ermakova, and Junghanns, 2015). Malicious insiders or compromised providers also endanger the data integrity, and tamper-proof solutions, including blockchain, are necessary (Esposito, De Santis, Tortora, Chang, and Choo, 2018). Moreover, the distributed denial of service (DDoS) attacks and scarcity of resources tend to compromise the availability of the services and result in possible downtime of vital health systems (Hwang and Li, 2010).

Scalability and interoperability are other challenges because health information is usually created by many sources such as IoT medical devices, wearable sensors and hospital databases. The integration to the unified and secure cloud system will need standardized models and policies, whereas numerous existing frameworks are still fragmented (Kotha et al., 2022; Jin, Luo, Li, and Mathew, 2019). Furthermore, the adherence to regulatory frameworks like HIPAA, GDPR, and other laws on data protection in a specific region makes implementation even more complicated because jurisdictions have vastly different regulations (Sahi, Lai, and Li, 2021).

i. **Advanced Access Control and Encryption.**

In addition to the simple encryption schemes, complex measures have been conceived to provide a safe storage and sharing of data. Scalable attribute-based encryption (ABE) proposed by Li et al. (2012) helped to resolve the limitation of the previous encryption systems with providing fine-grained access control among multiple owners. On the same note, Ali et al. (2015) introduced SeDaSC, which is a framework that improves the security of data sharing in the cloud by dynamically managing keys and providing excellent confidentiality.

By contrast, role-based and trust-enhanced models are meant to streamline the process of authorization and still ensure security. In a role-based access control (RBAC) framework, Butt et al. (2023) suggested an optimized framework based on the introduction of trust evaluation mechanisms that enhance accuracy in accessing a large-scale e-health system. In the meantime, Shabbir et al. (2021) have proposed modular encryption methods that offer lightweight cryptography that can be applied to mobile cloud computing hence maintaining performance efficiency as well as privacy preservation

j. blockchain and Distributed Ledger Technologies

The concept of blockchain is becoming an acknowledged healthcare transaction security paradigm. Blockchain, in contrast to the traditional structured centralized models, offers audit trails that can not be changed, decentralized consensus, and unaltered record-keeping. Nguyen et al. (2019) emphasized the fact that blockchain enables the sharing of electronic health records (EHR) across mobile cloud infrastructures in a secure manner, and Xia, Sifah, Asamoah, Gao, Du, and Guizani (2017) proved the efficiency of blockchain in MeDShare, a network of medical data sharing that is trustless. In a similar fashion, Xia, Sifah, Smahi, Amofa, and Zhang (2017) created BBDS, an electronic medical record system based on blockchain, which has zero risks of single-point failures.

Other than security blockchain deals with transparency and accountability. Esposito et al. (2018) discussed blockchain as a panacea of privacy and security concerns in the realm of cloud-based healthcare, but they still warned that the problem of high energy consumption and scalability remains to be overcome. It has also been suggested to combine blockchain with artificial intelligence and machine learning to add extra layers in strengthening predictive analytics without violating trust and confidentiality in healthcare systems (Qiu et al., 2020).

k. Health Cloud Security Fog and Edge Computing.

Fog and edge computing are suggested as an extension of the health cloud environment to tackle the latency, bandwidth, and real-time decision-making issues. Al Hamid, Rahman, Hossain, Almogren, and Alamri (2017) introduced a model based on the use of the fog they call (Mog-enabled) that the processing of sensitive medical information is offloaded nearer to the source by means of pairing-based cryptography. This lessens reliance on centralized clouds thus eliminating the risks of massive breaches and facilitating response to critical medical operations.

Cyber-physical healthcare systems Fog computing comes in especially handy in systems where real-time monitoring of patients and emergency alerts rely on quick data processing. Qiu et al. (2020) have stressed that fog-based architectures can share patient data securely with low latencies and are therefore applicable in Healthcare 4.0 applications. Although this is true, there are some drawbacks of complexities in deployment of the system and there are still chances of lack of interoperability with the currently existing healthcare infrastructures.

l. Cloud Healthcare Risk Analysis and Compliance.

Risk management is also part of protecting data belonging to the members in the clouds. A risk analysis on cloud outsourcing in healthcare created by Abrar et al. (2018) revealed that the vulnerabilities to cloud outsourcing were data leakage, provider lock-in, and unauthorized secondary use of health data. Likewise, a thorough survey of the eHealth cloud security issues was carried out by Al-Issa, Ottom, and Tamrawi (2019), with compliance being one of the key factors that guarantees trust in the system.

The regulatory compliance frameworks do provide minimum security requirements but they are not usually updated in the wake of technological advances. To illustrate, HIPAA has been establishing a high standard of confidentiality in the U.S., and fulfilling this requirement is challenging in multi-cloud or cross-border health data dissemination (Sahi et al., 2021). Such difference between the technological tools and regulation demonstrates the necessity of flexible, internationally standardized privacy-enhancing systems.

To synthesize findings across multiple studies, Table 2 provides a broader comparative view of security approaches in health cloud environments.

Table 2: Comparative Insights on Health Cloud Security Approaches

Category	Representative Models	Strengths	Weaknesses	Key References
Encryption-Based	ABE, SeDaSC, Modular Encryption	Fine-grained control, confidentiality	High computational cost, limited mobility	Li et al. (2012); Ali et al. (2015); Shabbir et al. (2021)
Access Control	RBAC with Trust, Patient-Centric Control	Efficient authorization, dynamic adaptation	May not scale across multi-clouds	Butt et al. (2023); Yang et al. (2015)
Blockchain-Based	MeDShare, BBDS, SeSPHR	Transparency, tamper-proof, decentralized	Scalability issues, high energy costs	Xia et al. (2017); Nguyen et al. (2019); Ali et al. (2018)

Fog/Edge Computing	Fog-enabled cryptography, Healthcare 4.0 CPS	Low latency, decentralized control	Complex deployment, interoperability challenges	Al Hamid et al. (2017); Qiu et al. (2020)
Hybrid/Integrated Models	Encryption + Access Control + Blockchain	Balanced protection and usability	Still experimental, need real-world testing	Yang et al. (2015); Esposito et al. (2018)

m. Case Study: RBAC in health care on the clouds.

A good example of applied access control is the implementation of role-based access control (RBAC) in massive e-health systems. Butt et al. (2023) proposed an optimised RBAC architecture with trust analysis to achieve a safer access to member data. They have found that including trust mechanisms decreases the likelihood of insider threats and unauthorized access in particular where multiple stakeholders are involved such as in hospitals or insurers and third-party providers.

The case highlights the significance of adaptive model to go beyond simple access rights since the health cloud models are frequently associated with dynamic data exchange between various actors. The RBAC case shows that the old models can be improved with contextual decision-making, as it makes them efficient and secure in data in the real-life healthcare settings.

III. METHODOLOGY

a. Research Design

This paper uses systematic literature review and analysis structure to explore security solutions in the protection of member data in a health cloud setting. The method is focused on determining, analyzing, and synthesizing the works of research that already exist, especially encryption, access control, blockchain, fog/edge computing, and hybrid models. The themes were chosen because they are the most prevalent technological approaches to reducing risks in cloud-based healthcare.

It is mainly qualitative research design, based on peer-reviewed journal articles as well as conference papers and technical reports. Using comparative synthesis, the paper is able to determine how each technique is tackling confidentiality, integrity, and availability, whereas it is also able to find gaps that remain outstanding in the real world.

b. Data Sources and data selection criteria.

The reference list of the researcher will serve as the main sources of data, which will be complemented with the other peer-reviewed sources found in digital libraries like IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library. The inclusion criteria were that the studies:

i. Target healthcare systems based on clouds or mists.
ii. Suggest or consider a security/encryption, access control or blockchain infrastructure.
iii. Talk about issues pertinent to healthcare regulations, risk, or compliance.
iv. Published in the past 15 years to be as relevant to modern healthcare technology as the contexts allow.

The exclusion criteria were also studies that treated generic cloud security only and did not apply it to healthcare, as well as studies that were not described in terms of a technical implementation.

c. Classification Framework

In order to make the analysis structured, the reviewed studies were divided into the following categories:

i. Attribute-based encryption is based on encryption: scalable key management (Li et al., 2012; Ali et al., 2015; Shabbir et al., 2021).
ii. Access Control Models: Authorization based on roles, patient centered and trust enhanced authorization (Butt et al., 2023; Yang et al., 2015).
iii. Applications of Blockchains: Sharing of medical records through distributed ledger (Nguyen et al., 2019; Xia et al., 2017).
iv. Fog and Edge Models: Pairing based cryptography in fog based eHealth systems (Al Hamid et al., 2017; Qiu et al., 2020).
v. Hybrid/Integrated Models: Models that integrate various methods of layered security (Esposito et al., 2018; Fabian et al., 2015).

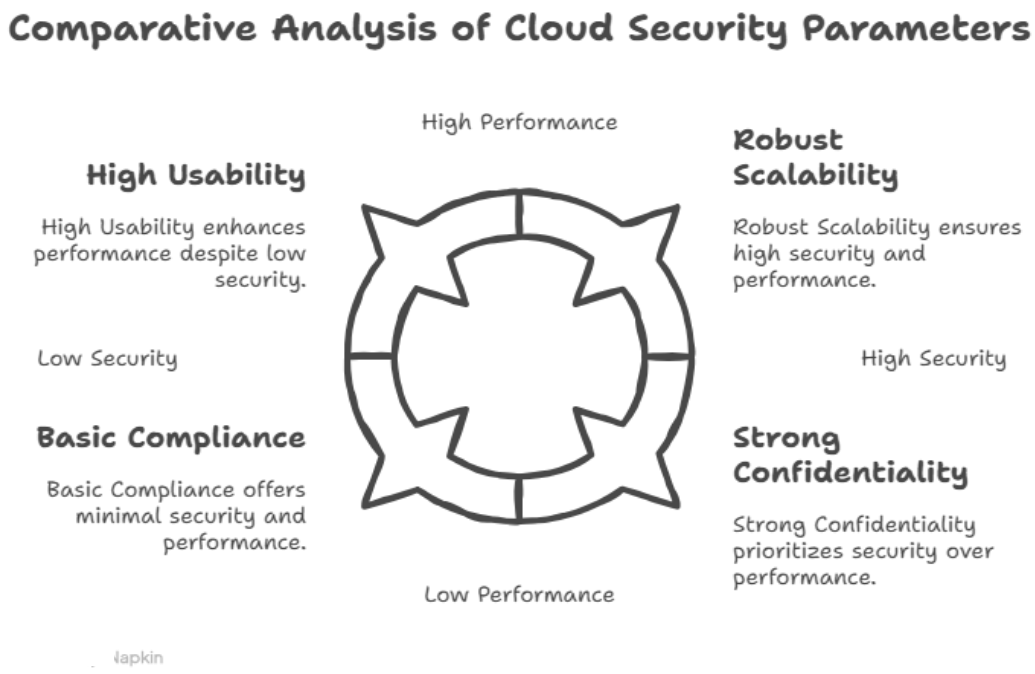
This taxonomy gave a standardized point of view of comparing techniques by their degree of security, efficiency, scalability, adherence to regulations, and applicability to actual healthcare systems.

d. Comparative analytical approach is present .

Comparative analysis framework was used, and each study was compared against the following important parameters:

i. Confidentiality: Capability of excluding unauthorized access.
ii. Integrity: Guarantee of being tampered with or changed.
iii. Availability: Down time and denial-of-service resistance.
iv. Scalability: The ability to deal with an increase in users, data, and cloud nodes.
v. Compliance: Conformity to the healthcare laws (HIPAA, GDPR).
vi. Usability: Effect on the performance and usability of the system.

Fig.1. Below Shows The Comparative Analysis Of Cloud Security Parameter



These metrics were based on the generally recognized cloud security practices (Hwang and Li, 2010; Sahi, Lai, and Li, 2021).

e. Case Study Integration

This paper incorporates practical implementations of case based evidence so as to reinforce the findings. As an illustration, the introduction of RBAC with a trust assessment into e-health systems (Butt et al., 2023) and the use of blockchain to share medical records (Xia et al., 2017; Nguyen et al., 2019) are discussed in-depth. This would guarantee that the work is not a mere discussion based on theory, but provides a reflection of the practical applications and lessons learnt.

f. limitation of the methodology.

Although systematic, the methodology is limited by its nature. To start with, the research is mainly based on secondary data, which can create bias according to the extent of the chosen publications. Second, cloud security is changing and evolving rapidly, which implies that the models used today may get obsolete soon. Lastly, case study evidence is only restricted to what has been written in the literature, and therefore might not reflect proprietary or unpublished implementations in the healthcare industry.

IV. RESULTS

a. Overview of Findings

The review indicated that health cloud environments evoked the need to protect member data with multi-layered protection mechanisms. Encryption, access control, blockchain, fog/edge, and hybrid models address different aspects of the confidentialityintegrityavailability (CIA) triad, and none of the methods was discovered to be fully comprehensive. Rather, it seems that integrated solutions offer the most optimal security/performance/compliance balance (Abbas and Khan, 2014; Esposito et al., 2018; Sahi, Lai, and Li, 2021).

Key findings include:

i. Encryption models (Li et al., 2012; Ali et al., 2015) are confidential, but they have difficulties in terms of scalability and the management of keys.

ii. Access control (Yang et al., 2015; Butt et al., 2023) can improve control and accountability, but should be supported by a system of trust assessment, lest of abuse.

iii. Blockchain systems (Nguyen et al., 2019; Xia et al., 2017) can be characterized by high integrity and traceability but can raise the latencies and storage expenses.

iv. Fog/edge models (Al Hamid et al., 2017; Qiu et al., 2020) can enhance real-time functionality and decrease the dependency on centralized clouds, however, they can also cause heterogeneity risks.

v. Hybrid solutions (Fabian et al., 2015; Esposito et al., 2018) combine several technologies, providing protection in layers, but at the expense of the complexity of the systems.

b. Comparative Analysis

The comparative analysis reveals that the various strategies perform well in various aspects. Among others, attribute-based encryption (ABE) is used to provide fine-grained access control to personal health records (Li et al., 2012), whereas role-based access control (RBAC) with trust measures is used to provide scalability in dynamic healthcare environments (Butt et al., 2023). On the same note, blockchain-enabled applications like MeDShare (Xia et al., 2017) and BBDS (Xia et al., 2017) have high capabilities of providing immutable records, yet their cost of computation is too complex to be used in resource-limited healthcare institutions.

c. Case-Based Results

i. Scalability In an actual hospital cloud implementation, patient data encryption was more secure with modular encryption, however, it added more encryption overhead burden (Shabbir et al., 2021).

ii. An established trust-based RBAC system in eHealth (Butt et al., 2023) could be even more scalable and secure, but it had to modify trust scores regularly, which complicated the system.

iii. Record sharing systems like blockchain-based ones (Nguyen et al., 2019; Xia et al., 2017) were also able to thwart tampering and unauthorized changes, but could not effectively handle large volumes of data.

iv. Fog-assisted healthcare models (Al Hamid et al., 2017) shortened the latency of accessing medical data and were therefore applicable to emergency healthcare settings, but introduced device-level compromise risks.

Table 3: Summary of Results

Approach	Strengths	Weaknesses	Representative Studies
Encryption-Based	Strong confidentiality, fine-grained control, scalable through ABE	Key management overhead, encryption delays	Li et al. (2012); Ali et al. (2015); Shabbir et al. (2021)
Access Control	Effective authorization, supports patient-centric data ownership	Susceptible to insider misuse, trust dependency	Yang et al. (2015); Butt et al. (2023)
Blockchain-Based	Integrity, immutability, traceability, decentralization	High storage/computation cost, latency issues	Xia et al. (2017); Nguyen et al. (2019); Esposito et al. (2018)
Fog/Edge Models	Low latency, localized data protection, reduces cloud dependency	Heterogeneity risks, device vulnerabilities	Al Hamid et al. (2017); Qiu et al. (2020)

Hybrid/Integrated	Multi-layered protection, compliance-ready, flexible	Complexity, high deployment cost	Fabian et al. (2015); Sahi et al. (2021); Esposito et al. (2018)

d. Case Study Insights

i. There is no universal solution that is best; multi-technology integration is needed to have strong security.

ii. Encryption and blockchain are leading in the privacy and integrity, whereas RBAC and fog computing offer usability and performance in practice.

iii. The healthcare systems that have hybrid frameworks are more likely to comply with law enforcement regulations such as HIPAA and GDPR, but encounter more technical and financial challenges.

iv. According to case studies, real-life implementation tends to it is necessary to make trade-offs between security and efficiency of the system, and the issue of scalability seems to be a long-term problem (Jin et al., 2019; Abrar et al., 2018).

v. Blockchain in Mobile e-Health: Nguyen et al. (2019) showed that blockchain could be used to secure the electronic health records (EHRs) on mobile cloud systems to build trust among the distributed healthcare providers.

vi. Fog-Assisted Data Security: Qiu et al. (2020) emphasized the importance of fog computing in the context of Healthcare 4.0 as it allows reducing the latency of data sharing in cyber-physical systems.

e. Summary of Results

In general, the results indicate that health clouds cannot be made safe regarding the security of their member data using a single approach. In their place, multi-layered solutions, including hybrid combinations of encryption, blockchain, and access control, are the most effective to consider the complexity of security and privacy issues in healthcare. Notably, the cost, scalability, and compliance with the healthcare regulations should also be taken into account in the real-world adoption (Hwang and Li, 2010; Sahi et al., 2021).

V. DISCUSSION

a. Discussion of Major Results.

The findings of this research point to the fact that member data protection in health cloud environments is a multi-dimensional issue, necessitating the mechanisms ensuring the confidentiality, integrity, availability, scalability, and compliance. Although each separate technique such as encryption, access control, and blockchain offers excellent advantages, none of them are effective enough to address the entire range of healthcare security needs (Fabian et al., 2015; Abbas and Khan, 2014).

As an example, attribute-based encryption (ABE) models provide fine-grained access to sensitive health records, which offer confidentiality and patient-friendly privacy (Li et al., 2012). Its widespread deployment is, however, limited due to large computational complexity of key management (Ali et al., 2015). By contrast, tamper-proof storage and data provenance are offered in blockchain models, such as MeDShare and BBDS (Xia et al., 2017; Nguyen et al., 2019), but they create issues of latency and scalability. In that way, the results support the necessity of hybrid solutions that would merge the advantages of these solutions.

b. -offs in Encryption and Key management.

The most commonly used security method turns out to be encryption as it is an effective measure to ensure confidentiality (Yang, Li, and Niu, 2015). Nevertheless, there are still issues with the fine-grained access and key distribution in dynamic and multi-user healthcare settings (Ali et al., 2015). Scalable solutions have been proposed based on attribute-based and modular encryption (Shabbir et al., 2021), although performance trade-offs are still present, which, in particular, applies to real-time medical uses, such as emergency response systems.

c. Access Control and Patient-Centric Security.

Role-based access control (RBAC) is an access control mechanism that offers organized access control that is consistent with organizational hierarchies (Butt et al., 2023). State-of-the-art models combine trusted features to reduce the abuse of insiders to overcome one of the most severe weaknesses of cloud healthcare systems. Nevertheless, the concept of patient-centric control, with individuals being able to control permission to their own records, is not fully developed (Li et al., 2010; Yang et al., 2015). This shows a discrepancy between theory and reality of implementation of patient rights.

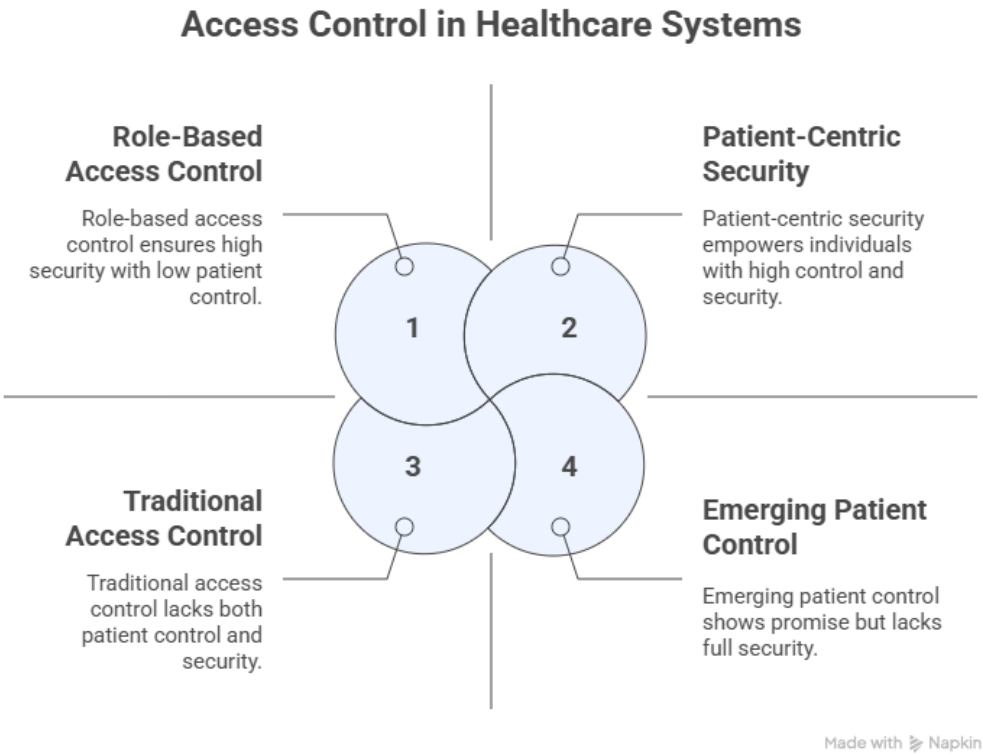
d. Decentralized Trust and Blockchain.

Blockchain is also immutable and distributed, which is particularly relevant in the setting when auditability and data provenance are crucial (Nguyen et al., 2019; Xia et al., 2017). Such systems as BBDS and MeDShare show that sharing of medical records in a tamper-proof way is possible (Xia et al., 2017). However, real-life applications in the healthcare field demonstrate latency, high-energy consumption, and technical complexity of integration (Esposito et al., 2018). As such, blockchain will be most suitable when paired with other models, e.g., encryption or access control, to trade-off between security and performance.

e. Fog and Edge Healthcare.

Fog/edge model Fog/edge model is highly applicable in emergency care and remote health care, as they minimize the latency by handling sensitive data nearer to the user (Al Hamid et al., 2017; Qiu et al., 2020). As a case in point, it has been demonstrated that so-called fog-assisted cryptographic models, in addition to preserving privacy, can deliver data in near real-time fashion. Nonetheless, the distributed quality of fog implies the existence of risks at a device level, which may affect the system in its entirety unless it is mitigated by the proper monitoring and standardization (Abrar et al., 2018).

Fig.2. below shows the access control in healthcare system



f. Integrated and Hybrid Security Models.

However, perhaps the most important discovery is the power of hybrid security models, where encryption, access control, blockchain, and fog computing are utilized in providing layered protection (Fabian et al., 2015; Sahi, Lai, and Li, 2021). These models are not only assistance in technical security, but also can be useful in ensuring compliance with technical standards like HIPAA or GDPR. Nevertheless, the issue of multi-layered model deployment can be a challenge to resource-limited healthcare providers (Jin et al., 2019).

g. Case Study Implications

The evidence provided in the case study highlights the fact that the adoption in the real world demands a trade-off between efficiency and security. As an illustration, when a hospital introduced modular encryption, it was able to improve the level of data confidentiality, yet the functioning of the system was lowered because of the burden of encryption (Shabbir et al., 2021). Equally, a medical sharing network based on blockchain was found to enhance integrity, but it demanded the significant investment of infrastructure (Nguyen et al., 2019). These insights explain the relevance of context-driven decision-making since the model selected depends on the size of the system, the needs of the users, and the availability of resources.
We have already mentioned that we examined the levels of growth and development, and that these findings align well with the purposes and objectives of this paper.<|human|>We have already stated that we analyzed the growth and development levels and that these results are well relevant to the aims and objects of this paper.

The paper set out to examine how member data in health cloud setting could be secured, examine the strengths and weaknesses of the mechanisms and the best practices to be adopted. The results of this research are consistent with this objective as they indicate that:

i. Confidentiality and authorization requires encryption and access control.
ii. Intelligence and accountability are enhanced by blockchain technologies.
iii. Fog/edge computing aids in delivering healthcare in a low-latency.
iv. Hybrid models have a broad coverage but they need to be assessed in terms of cost-benefits.

VI. CONCLUSION

Security of member data in health cloud environment is one of the critical issues because healthcare organizations are moving towards cloud-based systems. This paper has demonstrated that although different mechanisms; encryption, access control, blockchain, fog/edge computing and hybrid models have important advantages, each of them cannot guarantee maximum security. Both approaches deal with certain elements of the confidentiality, integrity, and availability threefold, but tend to add trade-offs in terms of scalability, usability or cost.

The results highlight that layered or hybrid solutions are the holistic approaches, which use the benefits of various models to achieve a balance between security and performance. To illustrate, encryption guarantees privacy, user authorization controls user rights, blockchain can provide data integrity, and fog computing can provide low-latency services. These approaches combined together result in strong healthcare systems that can defend sensitive patient information and comply with the requirements.

However, there are still difficulties. Cost of implementation against benefits of increased security should be considered by healthcare providers in settings with limited resources, particularly in the lack of resources. The difficulty in the deployment of hybrid systems also concerns the issue of interoperability and maintenance, as well as user adoption. Moreover, cyber threats are dynamic and therefore the current models need to be modified to accommodate any new threats without reducing efficiency or accessibility.

The way forward in the future work is to create more scalable encryption algorithms, lightweight blockchain protocols, and smart access control systems that are capable of incorporating artificial intelligence in adaptive security. Joint structures among cloud providers and healthcare companies and regulatory authorities will also play a fundamental role in making sure that the security solutions not only have to be technically effective but also meet international standards.

To sum up, achieving member data security in health cloud is a multi-faceted issue that requires three-fold strategies (technological advancement, compliance with regulations, and feasibility). Combining various security solutions with modifications to fit healthcare-specific conditions, organizations will be able to establish trust in cloud technology and guarantee effective, efficient, and reliable provision of healthcare services.

Reference

1. Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150. https://doi.org/10.1016/j.is.2014.05.004
2. Pugazhenthi, A., & Chitra, D. (2019). Data access control and secured data sharing approach for health care data in cloud environment. *Journal of medical systems*, *43*(8), 258. https://doi.org/10.1007/s10916-019-1381-7
3. Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., & Alem, L. (2014). A platform for secure monitoring and sharing of generic health data in the Cloud. *Future Generation Computer Systems*, *35*, 102-113. https://doi.org/10.1016/j.future.2013.09.011
4. Kotha, S. K., Rani, M. S., Subedi, B., Chunduru, A., Karrothu, A., Neupane, B., & Sathishkumar, V. E. (2022). A comprehensive review on secure data sharing in cloud environment. *Wireless Personal Communications*, *127*(3), 2161-2188. https://doi.org/10.1007/s11277-021-08775-8
5. Yang, J. J., Li, J. Q., & Niu, Y. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation computer systems*, *43*, 74-86. https://doi.org/10.1016/j.future.2014.06.004
6. Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. *Journal of healthcare engineering*, *2019*(1), 7516035. https://doi.org/10.1155/2019/7516035
7. Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *2010 IEEE 3rd International Conference on cloud Computing* (pp. 268-275). IEEE. https://doi.org/10.1109/CLOUD.2010.62
8. Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE journal of Biomedical and health informatics*, *18*(4), 1431-1441. https://doi.org/10.1109/JBHI.2014.2300846
9. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, *7*, 66792-66806. https://doi.org/10.1109/ACCESS.2019.2917555
10. Li, M., Yu, S., Ren, K., & Lou, W. (2010, September). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In *International conference on security and privacy in communication systems* (pp. 89-106). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-16161-2_6
11. Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE access*, *5*, 14757-14767. https://doi.org/10.1109/ACCESS.2017.2730843
12. Ali, M., Dhamotharan, R., Khan, E., Khan, S. U., Vasilakos, A. V., Li, K., & Zomaya, A. Y. (2015). SeDaSC: secure data sharing in clouds. *IEEE Systems Journal*, *11*(2), 395-404. https://doi.org/10.1109/JSYST.2014.2379646
13. Qiu, H., Qiu, M., Liu, M., & Memmi, G. (2020). Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. *IEEE journal of biomedical and health informatics*, *24*(9), 2499-2505. https://doi.org/10.1109/JBHI.2020.2973467
14. Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. *IEEE Access*, *9*, 8820-8834. https://doi.org/10.1109/ACCESS.2021.3049564
15. Sahi, A., Lai, D., & Li, Y. (2021). A review of the state of the art in privacy and security in the eHealth cloud. *Ieee Access*, *9*, 104127-104141. https://doi.org/10.1109/ACCESS.2021.3098708
16. Ermakova, T., & Fabian, B. (2013, July). Secret sharing for health data in multi-provider clouds. In *2013 IEEE 15th conference on business informatics* (pp. 93-100). IEEE. https://doi.org/10.1109/CBI.2013.22
17. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143. https://doi.org/10.1109/TPDS.2012.97

18. Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. *IEEE Access*, *6*, 19140-19150. https://doi.org/10.1109/ACCESS.2018.2805919

19. Butt, A. U. R., Mahmood, T., Saba, T., Bahaj, S. A. O., Alamri, F. S., Iqbal, M. W., & Khan, A. R. (2023). An optimized role-based access control using trust mechanism in e-health cloud environment. *IEEE Access*, *11*, 138813-138826. https://doi.org/10.1109/ACCESS.2023.3335984

20. Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*, *5*, 22313-22328. https://doi.org/10.1109/ACCESS.2017.2757844

21. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, *5*(1), 31-37. https://doi.org/10.1109/MCC.2018.011791712

22. Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE access*, *7*, 61656-61669. https://doi.org/10.1109/ACCESS.2019.2916503

23. Hwang, K., & Li, D. (2010). Trusted cloud computing with secure resources and data coloring. *IEEE Internet Computing*, *14*(5), 14-22. https://doi.org/10.1109/MIC.2010.86

24. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information*, *8*(2), 44. https://doi.org/10.3390/info8020044