Privacy Protection in Intelligent Healthcare Atomosphere: The Present and Prospect

Chandrhass Shankhdhar, L.S. Maurya

SRMS College of Engineering Technology, Lucknow

Corresponding author: Chandrhass Shankhdhar, Email: chandrahass.shankhdhar@srms.ac.in

The fast growth of Internet of Medical Things innovation has resulted in several breakthroughs in the smart healthcare field; it enhances healthcare systems to give more complex real-time services and more efficient patient motioning system. Nonetheless, despite Internet of Medical Things, there are the dazzling side, some problems continue to stymie its acceptance. In reality, collecting, transferring, storing, and utilizing data in medical applications raises concerns about privacy and data protection, particularly given the large number of parties involved throughout the data life cycle. Motivated by these facts, the purpose of this paper is to conduct a Systematic Literature Review of privacy-preserving methods employed in the smart healthcare ecosystem .A standardized Literature Review technique is used to choose current research publications published between 2017 and 2021 from several databases. Several papers were screened, and the selected papers were subjected to critical examination.

Keywords:Privacy Protection, E-Health Care, Internet of Medical Things (IoMT), Block Chain, Machine Learning.

2023. In Saroj Hiranwal & Garima Mathur (eds.), *Artificial Intelligence and Communication Technologies*, 461–465. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-955020-5-9-44

1 Introduction

A growing number of diseases can be prevented through smart healthcare, one of the fastest-growing technologies in recent years. IoMT is a network of medical devices, health systems, and services that are all interconnected. Connectivity, communication, captures, and exchange of Electronic Medical Records (EMRs) between entities is made possible by the IoMT [1] system. The EMR contains personal health information, whereas Internet of Things (IoT) implementations are often fraught with privacy and data security concerns. There are even more considerations when it comes to patient privacy. Because of this, people in the smart healthcare field are concerned about data security and privacy. Many people expect that their electronic medical records (EMRs), such as their blood group and pulse rate, can only be accessed by authorized health care providers and only with their permission or control. Researchers have recently shown an interest in preserving security and privacy in a smart healthcare setting. However, it is critical to be aware of the current IoMT system's security and privacy issues and it's solved by recent technology like block chain, big data and machine learning. Furthermore, it's important to know how effective the solutions that are being offered. In the literature, we found that these issues have received little attention. Consequently, a systematic literature review (SLR) is presented in this paper [2,3]. After the analysis of review we will find out the present scenario of privacy protection of the data.

2 Systematic Literature Review (SLR)

M. Tanriverdi [4] and other have introduced an efficient attribute-based encryption (ABE) system that out- sourced some encryption and decryption to the edge nodes and supports attribute modifications, allowing flexible control of the right of the user. This method has been tested and proven to be more efficient for re-source-constrained devices than the classic ABE method with respect to IoT-based smart healthcare [7]. It offers a solution that preserves privacy while also allowing patients to make pragmatic data sharing agreements with smart services by specifying the information that can be shared or used RFID authentication [5] scheme. By calculating the privacy risks associated with each data sharing, Alraja[6] et al. sought to safeguard the privacy of IoT users while also assisting them in reaching practical agreements with smart services and data consumers. Singh and Chatterjee developed an edge computing-based smart healthcare system with an intermediary layer dubbed the edge computing layer, which is responsible for controlling network latency and preservation patient data privacy. Fundamental security and privacy issues face the burgeoning healthcare industrial internet of things (HealthIIoT), such as safe fine-grained data transport, privacy preserving [7] keyword-based decryption, and malicious key delegation. In response to these problems, Sun et al. developed a Privacy-aware and Traceable Fine-grained System (PTFS) in cloud-assisted Health IoT[8], which provides safe fine-grained data transport, privacy-preserving data retrieval, efficient encryption, and decryption operations. For privacy in the smart healthcare environment, Sathya and Raja suggested a Euclidean L3P-PriSens-HSAC security framework. For the first time, a framework has been provided that provides enhanced privacy for RFID-based healthcare systems by integrating RFID authentication with access control approaches. A secure smart healthcare system defined by Zhang et al. offers user privacy protection by providing fine-grained access control to smart healthcare cloud data. Cipher text-policy attribute-based encryption is a promising cryptographic primitive [11].

3 Methodology

On the basic of proper review, analysis of the study is followed with various machine learning techniques and application of the black chain.

3.1 Decentralized Structural Design

Reading all primary research papers in this class, pertinent data was gathered. Each paper's major thesis is summarized in the section that follows. There is a need for a safe EHR management system for patients, doctors, and health service providers that are both regulated and secure, and this is what Chelladurai et al. recommended. The cryptographic hash functions used in the proposed system ensure high levels of security and integrity. Using the block chain, Lee et al presented a medical data preservation method for tele-care medical information systems (TMISs)[9] that includes a WBAN and a social network information transmission protocol. In order to safeguard patient privacy, Wang et al. presented a Double Block-chain Telemedicine Diagnosis (DBTMD)[10] method that creates a public chain called User chain and a consortium chain called Medical chain. Additionally, it creates an identity authentication chain to ensure that the doctor's identity information is always up to date. Using this research, keys' transaction costs can be reduced.

In addition, Wang et al. developed a low-cost fog computing-based data privacy protection, efficient retrieval, and analysis service for IoMT. There is a smart contract-enabled consortium block chain network built on the IPFS cluster node and smart contracts for patient and medical device authentication that was defined by Kumar et al. A contact tracing approach for 5G-integrated and Blockchain-based [14] medical apps has been presented by Zhang et al. This enables patients to be tracked and checked in a privacy-preserving manner as shown fig1. There is no need for an online registration centre with the computed transferrable authenticated key agreement technique defined by Wang et al. Certification and key escrow issues can be solved with certificate less public-key cryptography. Decentralized block-chain data privacy and sharing system GuardHealth was proposed by researchers Wang et al. [15] with the same goal in mind. Confidentiality, authentication, data preservation, and data sharing are all taken care of by the suggested system. Similarly, Dai et al. developed a block chain-enabled IoMT system to raise the level of security and privacy concerns of IoMTs. They also highlight the five various perspectives on the solutions given to COVID-19 by block chain-enabled IoMT.

E-Health block chain-based decentralized architecture was proposed by Uddin et al.. The sensing layer (Body Area Sensor Network), the NEAR processing layer (the Fog), and the FAR processing layer compose this architecture's three levels (the Cloud). Access control is fine-grained and flexible, with revocability of consent, audit ability, and tamper resistance. Block chain-based smart healthcare systems (SHS) developed by Tripathi et al aim to provide the system with inherent security and integrity. This is known as the Smart and Secured Healthcare System (S2HS).

The Hyper ledger permission block chain technology, developed by Usman and Qamar, is used to maintain and share electronic medical records in a secure and efficient manner (EMRs). Patient-centered block chain framework Health Chain was introduced by Hylock and Zeng in a research article to promote immutable log keeping, encourage patient involvement and facilitate safe and secure flow of data between patients and providers. The current options for retrieving electronic medical records either fail to protect sensitive data or are limited to a single picture data source. Blockchain-based medical encrypted image retrieval is a solution to these issues, as described by Shen et al. [12,13]. With the help of block chain technology, they demonstrated the suggested scheme's layered architecture and threat model. Health data are encrypted and used for fine-grained access control in the Health chain system, which was developed in a study by Xu et al. to preserve the privacy of large-scale health data.

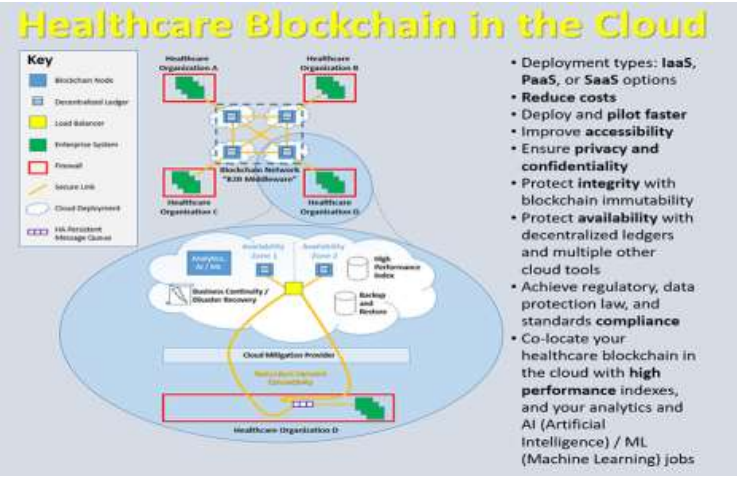

Fig1: Decentralized healthcare systems

4 Discussion and Future Direction

Decentralized healthcare systems shown in fig1, such as mobile and smart IoT solutions, are being prioritized above traditional health infrastructures because they ensure that patients receive healthcare services more quickly and efficiently. In spite of this, as shown throughout the proposed SLR, there remain issues to address, primarily the absence of a comprehensive strategy that takes privacy into account throughout the data lifecycle and the requirements of stakeholders. It's considerably more difficult to keep patients' sensitive data safe from unauthorized access because privacy must be considered at every stage of data collection, transport, use, and storage. However, what if we took privacy into account even before coming up with these clever and unique solutions, Rather than focusing on improving the actual smart IoT-based healthcare solutions, why not emphasize the necessity of privacy before they even exist? Prior to the development of smart solutions, we believe that privacy and feasible best practices for preserving it should be considered.

5 Conclusion

There was a comprehensive review of the existing privacy-preserving solutions in the smart healthcare environment undertaken as a part of this paper, which we called a Systematic Literature Review (SLR). Several components of the original studies' material, including the privacy mechanisms utilized, privacy principles, IoMT architecture, stakeholder requirements, etc. were analyzed to address the study questions. More than 70 percent of primary studies surveyed neglected the needs of stakeholders, particularly patient privacy preferences and privacy laws; in addition, the data collection phase is the least considered, which translates the neglecting of the two criteria: data collection limitation and data minimization. As noted in the preceding sections, a lack of a holistic strategy to ensuring privacy throughout the data life cycle and in accordance with the interests of many stakeholders is evident. Accordingly, we hope that our systematic review will serve as a valuable resource for academics who are concerned with preserving the privacy of Internet of Things (IoT) devices and services. In our current research, we intend to present a block chain-based solution for privacy-preserving in IoMT that overcomes the constraints of the prior methods and considers the whole privacy elements embraced in the previous analysis, to assure comprehensive privacy and security coverage.

References

[1] N. Dilawar, M. Rizwan, and F. Ahmad, "Blockchain: securing internet of medical things (IoMT)," International Journal of Advanced Computer Science and Applications, vol. 10, no. 1, pp. 31, 2019.
[2] Y. Xiao and M. Watson, "Guidance on conducting a sys- tematic literature review," Journal of Planning Education and Research, vol. 39, no. 1, pp. 93–112, 2019.
[3] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the in- ternet of medical things; the role of machine learning ap- proaches," Peer J Comput. Sci.vol. 7, pp. 414, 2021.
[4] M. Tanriverdi, "A systematic review of privacy preserving healthcare data sharing on blockchain," Journal of Cyber- security and Information Management, vol. 5, pp. 31–37, 2020.
[5] L. H. Iwaya, A. Ahmad, and M. A. Babar, "Security and privacy for mHealth and uHealth systems: a systematic mapping study," IEEE Access, vol. 8, pp. 150081–150112, 2020.
[6] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," Computer Communications, vol. 153, pp. 311–335, 2020.
[7] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical internet of things: a review," Security and Communication Networks, vol. 2018, Article ID e5978636, pp9-12, 2018.
[8] Z. El Ouazzani, H. El Bakkali, and S. Sadki, "Privacy pre- serving in digital health: main issues, technologies, and solutions," Research Anthology on Privatizing and Securing Data, IGI Global, Hershey, Pennsylvania, pp. 1503–1526, 2021.
[9] W. Fang, X. Z. Wen, Y. Zheng, and M. Zhou, "A survey of big data security and privacy preserving," IETE Technical Re- view, vol. 34, no. 5, pp. 544–560, 2017.
[10] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," Journal of Medical Systems, vol. 41, no. 8, pp. 127, 2017.
[11] Z. El Ouazzani and H. El Bakkali, "A classification of non- cryptographic anonymization techniques ensuring privacy in big data," International Journal of Communication Networks and Information Security, vol. 12, pp. 142–152, 2020.
[12] D. Preethi, N. Khare, and B. K. Tripathy, "Security and privacy issues in blockchain technology," in Blockchain Technology and the Internet of Things, Apple Academic Press, New Jersey, NJ, USA, vol24, pp45-87, 2020.
[13] Risk Based Security, "2021 Midyear data breach QuickView report," Risk Based Security, Richmond,VA,USA,https://pages.riskbasedsecurity.com/hubfs/Reports/2021/2021%20 Mid%20Year%20Data%20Breach%20QuickView%20Repor t.pdf, 2021.
[14] M. Verdonck and G. Poels, "Decentralized Data Access with IPFS and Smart Contract Permission Management for Electronic Health Records," in Proceedings of the International Conference on Business Process Management, Rome, Italy, pp-120-128, September 2021.
[15] G. Eysenbach, "What is e-health?" Journal of Medical In- ternet Research, vol. 3, no. 2, pp. 833, 2001.