Engineering and Scientific International Journal (ESIJ)
Volume 11, Issue 2, April – June 2024
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Ensuring the Security and Efficiency of Fog- Assisted IOT Cloud Based Electronic Medical Records Sharing through Lightweight Blockchain- based Access control

S.J.Sujitha[#1], Dr. Tamilselvi.P[*2]
[1]*Research Scholar,* [2]*Assistant Professor*
[1,2]*Department of Computer Science, VELS Institute of Science and Technology, Tamil Nadu, India*

Abstract — The handling and accessibility of Electronic Medical Records (EMRs) have been completely transformed by the growing integration of cloud computing and Internet of Things (IoT) technologies in the healthcare industry. This research presents a new method for implementing a lightweight blockchain-based access control system to meet the critical security and efficiency concerns in the sharing of fog- assisted IoT cloud-based EMRs. Thanks to the integration of data from several medical treatment applications and Internet of Things devices, the outsourcing of encrypted electronic medical records (EMRs) has become a fundamental aspect of the modern healthcare scene. This strategy has unmatched benefits, such as increased accessibility, efficient inter-professional collaboration, and a significant decrease in computational operation expenses. The goal of this research project is to maximise the effectiveness of EMR sharing while simultaneously strengthening the security of sensitive medical data. The suggested framework makes use of blockchain technology to provide a simple and safe access control system for the Internet of Things with assistance from Fog. By doing this, the system delivers strong resistance to unwanted access, transparent access, and data integrity.

Keywords: *Privacy Preservation; Blockchain Security; Increasing Efficiency.*

1. Introduction

Protecting sensitive medical data, especially Electronic Medical Records (EMRs), has become a critical responsibility in the field of healthcare informatics. Because medical data is sensitive and private, it needs to be protected with robust methods that both thwart possible attacks and enable safe sharing between authorised bodies. The Internet of Things (IoT) is driving the creation of comprehensive and effective EMRs. These gadgets, which are outfitted with advanced sensors, are essential for tracking, identifying, gathering, and communicating patient health data in real time. The introduction of IoT devices in healthcare raises issues with data security and sharing effectiveness notwithstanding its revolutionary influence. In particular, in Fog-assisted IoT cloud environments, the necessity to create a system that strengthens medical data security while also optimising EMR sharing efficiency is driving this research endeavour. Addressing the risks of data loss, unauthorised access, and unintentional exposures requires a targeted strategy. In order to create a safe and effective environment for exchanging EMRs, the suggested architecture takes advantage of the synergies between lightweight blockchain-based access control and fog-assisted IoT. By means of this integration, the solution preserves the integrity and openness of the whole data sharing process while guaranteeing the privacy of sensitive medical data. This study advances secure healthcare by examining the complex interactions between IoT devices, medical data security, and cutting-edge blockchain technology.

2. Related Work

Regarding the development of IoT and cloud computing in the healthcare industry, high accessibility, efficient collaboration, and no computational operation cost are made possible by outsourcing encrypted Electronic medical records (EMRs) that are generated by the combination of health data gathered from IoT devices and medical treatment applications. The privacy of the best EMRs, which are encrypted using safe and lightweight cryptographic protocols before being outsourced to the cloud, is a common worry in current applications and research projects. The security and privacy of the data gathered by IoT devices, where the sent data may be compromised before it is aggregated, are not taken into account by this method. Moreover, the privacy of IoT data transmission and aggregation, outsourced encryption, and policy updates have not been handled by current IoT-cloud based access control solutions. Lastly, we ran experiments to assess the effectiveness of our scheme and associated works and carried out the comparison analysis to show the computation cost. Because our system produced the lowest processing cost for both encryption and decryption at end-users' devices, the experimental results demonstrated its superior performance over previous works.

[2] Applications for smart remote healthcare are growing at a rapid pace thanks to IoT. For patients with chronic illnesses or those who are at danger, these Internet of Things-based remote healthcare applications provide prompt and preventive medical care. However, a major

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

worry in remote healthcare applications continues to be protecting patient privacy and data security while transmitting sensitive medical data among medical IoT devices. Medicinal data that has been tampered with or corrupted might lead to incorrect diagnosis and serious health problems. It's also necessary to address and enhance the responsiveness and efficiency of the current remote medical apps. In view of the requirement for safe and effective patient care, this article suggests a lightweight, Blockchain-based, Fog-enabled remote patient monitoring system that offers excellent security and quick reaction times.

By providing constant, round-the-clock surveillance without expensive and limited human resources and with a low mistake rate, the Internet of Things (IoT) has completely changed the way patient data and healthcare monitoring are captured and monitored. Utilising medical equipment as objects or nodes to enable efficient and economical patient monitoring and recording, the Internet of Medical objects (IoMT) is a subset of the Internet of Things (IoT). Observing patients in hospitals, keeping an eye on patients in their homes, and helping physicians and nurses evaluate patients' health conditions on a regular basis and send out warning signals when emergency treatment is required are just a few of the many issues that the IoMT can handle.

In order to support the execution of various latency-sensitive and computationally demanding Internet of Things (IoT) applications, there has been a recent emphasis on the integration of Edge, Fog, and Cloud infrastructures. While several real- world frameworks make an effort to support this kind of integration, they are limited in terms of resource management, platform independence, security, and multi-application execution. We suggest an architecture called FogBus that enables end-to-end IoT-Fog(Edge)-Cloud integration in order to overcome these constraints. FogBus provides execution and interaction interfaces for IoT applications and compute instances that are independent of platforms. It lets service providers manage their resources and customers run numerous applications at once in addition to developers building applications. Additionally, FogBus uses encryption, blockchain, and authentication methods to safeguard critical data processes.

Due to the Internet of Things' (IoT) quick development, wireless body area networks' (WBANs) common use in smart healthcare has attracted interest from a broad range of societal segments. In this work, the sophisticated technologies of fog computing, software-defined networking (SDN), and blockchain are utilised to alleviate the pressing issues, which include resource restrictions, low-latency service supply, mass data processing, strict security standards, and the absence of a central organisation. These technologies serve as the foundation for a task offloading method called LSRDM-EH, which enables resource-constrained edge devices to perform job offloading through centralised low- latency, secure, and reliable decision-making algorithm with strong emergency handling capabilities. Furthermore, a thorough blockchain-based two-layer and multidimensional security system is required to guarantee the safety of the entire network.

3. Existing System

Although there have been notable advancements in IoT-cloud based access control systems recently, there are still major obstacles in the way of creating a thorough and cohesive framework for the efficient and safe exchange of Electronic Medical Records (EMRs). Notably, the privacy of IoT data transmission and aggregation, outsourced encryption, and the dynamic policy updates necessary for efficiently regulating EMRs have proven to be challenging for current systems to handle. When it comes to access control systems for healthcare data—especially electronic medical records—current solutions have showed potential in some areas but have frequently failed to offer a comprehensive and unified strategy.

A significant drawback is the disjointed handling of security issues related to external encryption. Although current solutions have made progress in mitigating this issue, a more cohesive and comprehensive strategy is still required to protect data privacy throughout the intricate web of linked devices. Another important aspect that current systems have struggled to fully handle is policy modifications for EMRs. Because healthcare laws and policies are always changing, it is necessary to have a system that can easily adjust to new developments in order to keep access control measures current and compliant with new requirements. Many of the systems in use today are not flexible enough to apply adjustments to policies in real time, which can result in vulnerabilities and non-compliance. While some of the current technologies have shown efficiency advantages by lowering the processing costs associated with encryption and decryption at the end- users' devices, these strategies may not always be feasible.

While lower processing costs are a good thing, they don't always convert into comprehensive and workable plans that can successfully negotiate the complex world of EMR sharing. In conclusion, the current system landscape shows that while some parts of EMR sharing have been addressed admirably, a unified, safe, and effective solution has not been provided. Because of the fragmented nature of existing methods, a more cohesive solution is required, one that can easily integrate outsourced encryption, protect the privacy of IoT data transfer and aggregation, and enable dynamic policy modifications for EMRs. The goal of this study is to build a bridge.

DOI: **10.30726/esij/v11.i2.2024.112004**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

4. Proposed Modelling

We provide an inventive access control technique called Light MED in response to the difficulties and constraints found in the current systems. The purpose of this suggested system is to provide cloud-based, secure, scalable, and fine-grained Electronic Medical Records (EMRs) sharing that is seamlessly connected with blockchain, fog computing, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). By tackling the crucial issues of security, efficiency, and scalability, Light MED seeks to transform the EMR sharing environment as a comprehensive solution.Security, granularity, and scalability are the cornerstones of the suggested Light MED access control system. Light MED makes use of the interplay of fog computing, CP-ABE, and blockchain to guarantee safe and granular access to EMRs, enabling precise control over data accessible. Because of its smooth scalability, this programme can easily meet the increasing needs of healthcare data sharing in a constantly changing, networked setting.Healthcare data security and efficiency are being revolutionised by the integration of Lightweight Blockchain-Based Access Control into Fog-Assisted IoT Cloud-Based Electronic Medical Records (EMRs) Sharing. This integration offers numerous benefits. Assurance of Data Integrity: The fundamental strength of blockchain technology is its unmatched capacity to guarantee data integrity. Blockchain acts as a tamper-resistant ledger in the healthcare industry, where patient information authenticity and accuracy are non-negotiable. Every EMR transaction is safely recorded in an unchangeable chain of blocks and cryptographically hashed. This ensures that data is permanently committed to the blockchain, resulting in an irreversible record of patient health information.

5. System Architecture

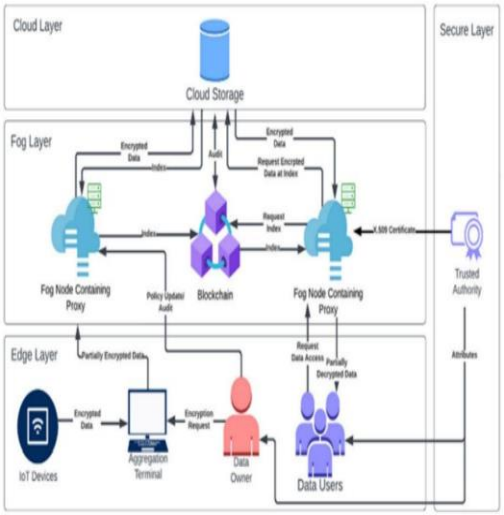

Fig.1: System architecture

Guaranteeing the Security and Effectiveness of IoT Cloud-Based Fog-Assisted Electronic Medical Records (EMRs) Coordination of multiple separate modules, each providing crucial functions to the system as a whole, is required for sharing via Lightweight Blockchain-Based Access Control.

6. Modules

6.1 Data Owner Module

This system's fundamental component is the Data Owner module. The role of Data Owners is crucial in the field of healthcare informatics, as sensitive patient data is frequently generated and updated. It is the duty of these organisations, which are frequently healthcare facilities or professionals, to create and maintain Electronic Medical Records (EMRs). The module is distinguished by its capacity to specify the properties required for accessing various types of medical data, allowing for the elaborate definition of access controls. Applying Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is how this process is carried out. EMRs that are encrypted are converted into ciphertexts with access controls associated with particular attributes by the Data Owner module. For safekeeping and effective sharing, this encrypted data is then contracted out to the Cloud Storage module.

6.2 Data User Module

The Data User module is used to represent people or organisations requesting access to the encrypted EMRs. Healthcare providers, approved researchers, and even patients themselves may be considered among these entities. Not everyone has access to medical records; Data Owners have established predetermined policies that control access. Access to certain medical records can only be requested by those who meet the requirements of the privacy- preserving access policy system, which is mainly enabled by CP-ABE. The system verifies the user'sattributes against the preset policies once the module starts the access request process. Data Users are granted authorised access to the EMRs upon successful verification, guaranteeing that only individuals with the necessary credentials and valid reasons can access sensitive medical data.

6.3 Cloud Storage Module

The encrypted and outsourced EMRs are stored securely in the Cloud Storage module. Cloud storage is essential in a fog-assisted Internet of Things cloud-based system where data transmission is decentralised and dynamic. This module makes sure that data is stored in a secure and private manner after it is encrypted and received from Data Owners. EMRs can be securely stored in a scalable and easily accessible environment thanks to cloud storage,

DOI: **10.30726/esij/v11.i2.2024.112004**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

which serves as a decentralised data hub. By utilising blockchain technology, it improves data integrity and makes sure that medical records are always easily accessible to authorised parties and resistant to tampering. This joint endeavour by Cloud Storage and the blockchain creates a strong basis for the safe and effective exchange of EMRs.

6.4 Trusted Authority Module

The module for trusted authority acts as the protector of access policies that protect privacy. In order to verify access policies against user attributes throughout the encryption and decryption procedures, it plays a crucial role in the implementation of CP-ABE. As an arbiter, the Trusted Authority module makes sure that access controls are constantly followed and that only authorised users possessing the necessary characteristics are able to decrypt particular EMRs. This module works closely with Data Owners to ensure the security and privacy of sensitive medical data while verifying access requests. The additional layer of trust and verification that the Trusted Authority module provides strengthens the fine- grained access control techniques.

6.5 IoT Device Module

The networked devices with sensors and monitoring features that help create Electronic Medical Records (EMRs) that are updated in real time are represented by the IoT Device module. These gadgets are essential for gathering health- related data in fog-assisted IoT cloud-based systems. The module adds to the dynamic aspect of the EMRs by ensuring the continual capture and transmission of patient health conditions. In tight partnership with Fog Nodes, the IoT Device module enables safe data transmission and aggregation, guaranteeing that the records generated are precise, timely, and appropriately represent the patient's health state. The constant flow of data improves the EMR system's overall effectiveness.

7. Future Enhancement

Addressing the issues surrounding healthcare data sharing has advanced significantly with the implementation of Lightweight Blockchain-Based Access Control to Ensure the Security and Efficiency of Fog-Assisted IoT Cloud-Based Electronic Medical Records Sharing. With that in mind, we will concentrate our future efforts on two main areas: integrating fog computing and putting attributes concealing into practice to make the most out of the system. Attributes Hiding: Including attributes hiding in the access control mechanism is one of the important issues we intend to tackle in our upcoming work. As of right now, the programme uses an access policy structure that protects privacy, guaranteeing that only individuals who meet the requirements can view particular medical records. Aspects concealment, which enables Data Owners to designate properties that stay hidden during access requests, may be improved upon, nonetheless. The method of access control is made more granular by attributes concealing. Data Owners can now carefully decide which qualities to display and which to remain hidden thanks to this improvement. When handling sensitive patient data,this capacity becomes more important.

7.1 Integration of Fog Computing

Another direction for our future research is to fully leverage Fog Computing to improve the system's responsiveness and efficiency. By putting the cloud closer to the network's edge, fog computing marks a paradigm shift in how computational resources are distributed. Our plan includes Fog Computing in order to maximise resource utilisation and enhance the overall efficacy of Electronic Medical Records (EMRs) sharing. By intelligently pooling resources and dynamically offloading computational tasks to neighbouring Fog Nodes, fog computing is made possible. Significantly less latency in data processing and transmission may result from this decentralised approach to computer resources. Its optimisation becomes even more important in an IoT context that uses fog assistance, where real-time data is critical.

8. Conclusion

In conclusion, the suggested Light MED scheme through Lightweight Blockchain-Based Access Control represents a major development in tackling the dual difficulties of efficiency and security in Fog-Assisted IoT Cloud-Based Electronic Medical Records (EMRs) Sharing. Using the advantages of blockchain technology and fog computing, this creative plan has been developed to offer lightweight, fine-grained, and secure access control for outsourced IoT-EMRs. Our plan lays the foundation for a strong and private-preserving access control system by introducing a revolutionary method to IoT data encryption and secure aggregation. The complete outsourcing of the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) encryption and decryption procedures to fog nodes is one of the main contributions of the Light MED method.In addition to guaranteeing lightweight and fine-grained data access, this strategic outsourcing dramatically lowers the total communication and computation costs for end users and data owners. The granularity of access control is improved by the combination of CP-ABE with privacy-preserving rules, which enables Data Owners to establish complex policies while protecting patient privacy. This is especially important in the healthcare industry, where sensitive medical data demands a careful, privacy- focused approach. Our plan provides tamper- resistant and decentralised storage by utilising blockchain technology, guaranteeing the availability and integrity of EMRs.Our method relies heavily on the fog

DOI: **10.30726/esij/v11.i2.2024.112004**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

computing concept, which allows for intelligent resource sharing and dynamic offloading of computational jobs to adjacent fog nodes. By optimising data processing and transmission, this decentralised solution solves the efficiency issues that arise in fog-assisted Internet of Things environments. By intelligently dividing computational duties, the integration of fog computing not only improves the responsiveness of the system but also helps to maximise resource efficiency. To summarise, the Light MED scheme offers a comprehensive resolution to the complex problems related to the security and effectiveness of exchanging IoT cloud-based EMRs with fog assistance. Our plan is a cutting-edge strategy that is in line with the changing needs of healthcare data management because it entirely outsources CP-ABE operations, includes privacy-preserving measures, and integrates fog computing and blockchain.

References

[1] U. C. Yadav and S. T. Ali, "Ciphertext policy- hiding attributebased encryption," in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Aug. 2015, pp. 2067-2071, doi:10.1109/ICACCI. 2015.7275921.
[2] P. Sanchol, S. Fugkeaw, and H. Sato, "A mobile cloud-based access control with efficiently outsourced decryption," in Proc. 10th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud), Aug. 2022, pp. 1-8, doi: 10.1109/MobileCloud55333.2022.00008.
[3] C. Hahn, J. Kim, H. Kwon, and J. Hur, "Efficient IoT management with resilience to unauthorized access to cloud storage," IEEE Trans. Cloud Comput., vol. 10, no. 2, pp. 1008-1020, Apr. 2022, doi: 10.1109/TCC.2020.2985046.
[4] Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15), 7912.
[5] Huang, Q. (2020).. Computers & Security, 99, 102010.
[6] Sun, X., & Huang, Q. (2020). A blockchain- based scheme for privacy-preserving and secure sharing of medical data. Computers & Security, 99, 102010.
[7] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, December).
[8] Tanr?verdi, M. (2020). A systematic review of privacy-preserving healthcare data sharing on blockchain. J Cybersecur Inf Manag, 5(2 SI 1), 31-
[9] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework.
[10] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43, 1-9.
[11] Sharma, P., Borah, M. D., & Namasudra, S. (2021). Improving security of medical big data by using Blockchain technology. Computers & Electrical Engineering, 96, 107529.
[12] Liu, X., Wang, Z., Jin, C., Li, F., & Li G. (2019). A blockchain-based medical data sharing and protection scheme
[13] Tian, H., He, J., & Ding, Y. (2019). Medical data management on blockchain with privacy. Journal of medical systems, 43, 1-6.
[14] Wang, B., & Li, Z. (2021). Healthchain: A Future Internet, 13(10), 247.
[15] Gao, F., Tao, X., & Liu, S. (2018). Blockchain- based data preservation system for medical data. Journal of medical systems, 42, 1-13.
[16] Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. Applied Sciences, 12(15), 7912.
[17] A case study on blockchain technology in healthcare: MedRec, a, A., Aria, A., and Halamka,
[18] J.D. In: 2016 IEEE Open&BigData Conference
[19] FoxNewsHealth: Hospitals Throughout England Are Hit by a "Ransomware" Cyberattack. Associated Press, May 2017
[20] Glaser, A.: The global ransomware attack-
[21] Recode has affected US hospitals (2017). Global EU cyberattack: hackers target NSA hospitals, according to Recode.net/2017/6/27/15881666
[22] Gul, O.; Al-Qutayri, M.; Yeun, C.Y.: The structure of an electronic health record system at the national level. In: 2012's Cloud Computing
[23] Hendrick, E., Schooley, B., Gao, C.: CloudHealth: Creating a Sturdy Cloud Platform for Applications in Healthcare. In: IEEE 2013's 10th Conference on Consumer.