10.48047/jocaaa.2024.33.06.30

EFFICIENT AND SECURE BLOCKCHAIN-BASED ACCESS CONTROL FOR FOG-ASSISTED IOT CLOUD IN ELECTRONIC MEDICAL RECORDS SHARING

S.Swetha.[1], Ms.Ch.Ananya[2], Ms.G.Bhanusha[3], Ms.Y.Anjali[4]
[1]Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad
Email:swecswetha@gmail.com

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT:

As IoT devices proliferate and healthcare organizations need more efficient ways to share patient data, fog-assisted IoT cloud environments have arisen. In such setups, it becomes critical to handle access control to sensitive data effectively and securely, including Electronic Medical Records (EMRs). We tackle this challenge creatively using the Efficient and Secure Blockchain-Based Access Control (ESBAC) framework, which is built for Fog-assisted IoT Cloud situations in EMR sharing. The ESBAC design incorporates the immutability and transparency of the blockchain to provide trustworthy auditability and access control. Participants in the installation of a consortium blockchain include authorized entities, patients, and healthcare professionals. To guarantee that no unauthorised parties may see or make changes to patient records, every electronic medical record (EMR) contains a smart contract that details who can access what and how. Security and privacy are enhanced because to the blockchain's decentralization, which prevents any one entity from exerting excessive influence. To strike a reasonable balance between speed and security, the suggested system employs attribute-based access control in conjunction with lightweight encryption techniques. This allows for very granular access control rules to be implemented with very little computational burden. The proposed approach is tested and compared to existing techniques using thorough simulations. The results demonstrate that ESBAC significantly reduces access latency and enhances security in EMR sharing. .

Features: small size Access Control, Blockchain, Encryption, Internet of Things Fog Layer, Medical Record

INTRODUCTION

Electronic medical records include patients' private and sensitive information such as medical histories, diagnoses, and treatment plans. Protecting the privacy of patients and complying with regulations like as HIPAA need strict measures to ensure the security of this information. Quick access to relevant EMRs is essential for healthcare providers, authorized personnel, and patients to make informed decisions. When it comes to the complexity of IoT Cloud settings, standard access control methods like role-based access control fall short. This is because these environments are constantly changing and consist of different types of data. As a possible paradigm shift, fog computing has the ability to solve the problems of latency, bandwidth, and real-time processing that plague IoT networks. Installing fog nodes close to the network's edge allows for processing data closer to its source, which improves responsiveness and reduces latency. Because timely access to patient data may affect clinical decisions, this design is particularly significant for healthcare applications. Problems

including node heterogeneity and changing network circumstances have emerged as a result of incorporating fog computing into the access control system, and they must be addressed if efficiency and security are to be preserved. The inherent properties of blockchain technology—its transparency, immutability, and decentralised

consensus—have garnered significant interest. It is an excellent material for making secure, impenetrable access control systems because of these qualities. By providing a verifiable and traceable record of access events, blockchain technology has the potential to improve transparency and responsibility in electronic medical record (EMR) sharing. Each electronic medical record (EMR) may have granular control over data access by attaching a smart contract that sets access limitations based on the requesting entity's attributes. Data mining plays a crucial role in the development of the digital economy in many industries and business types [1]. The sources of this data include healthcare, smart cities, and smart agriculture, among other smart technology applications. Nevertheless, there is still a need for study into how to keep data mining information private and secure. One notable use of IoT in smart healthcare is the monitoring of patients' vital signs via the use of wearable sensors and devices [2].The research presented in [3] aimed to address intrusion and security concerns, in contrast. Their proposed solution integrates blockchain technology with the Internet of Things (IoT) architecture, using a bio-sensor to gather real-time patient health data that is then stored securely on the blockchain. Importantly, this biosensor technology allows for exact, tamper-proof data storage, which is crucial considering the sensitivity of the produced personal information. Nevertheless, this approach does not take into account the user's current location and has latency issues. The cloud is a common place for traditional smart health ecosystems to store and analyze data [4].Additionally, these centralized cloud solutions are not suitable for situations that need quick responses. In cases when time is of the essence, such as during a heart attack, immediate access to patient records is crucial [5]. The overarching objective of this project is to design, develop, and assess an ESBAC framework tailored to EMR sharing in Fog-assisted IoT Cloud environments. The framework tackles the following significant problems:A high level of efficiency: In order to ensure that EMRs are accessible in a timely manner, the access control mechanism must be able to handle the possible overhead of blockchain consensus techniques and the distributed nature of fog computing. Finding the sweet spot between efficiency and safety is of the utmost importance.Ensuring the integrity of data and safeguarding patient privacy are of the highest priority in terms of security. Strong authentication, authorization, and encryption techniques are essential for the framework to prevent unauthorised access, manipulation, and data breaches.•The network environment, device capabilities, and data relevance of fog-assisted IoT cloud systems are inherently changing. The architecture has to adapt to these changes while keeping its security assurances.With the proliferation of Internet of Things (IoT) devices and electronic medical records (EMRs), the need for access control services is only going to rise. To keep up with this demand, the framework must be scalable.

Contribution: By releasing a state-of-the-art plan to solve the aforementioned problems, we integrate blockchain technology, fog computing, and adaptive consensus mechanisms: . Health information technology (IoT) and access control are two areas that can benefit from this research. •With Fog's help, the ESBAC framework should provide a thorough answer to the problem of access control in IoT cloud settings, allowing for the secure and effective exchange of electronic medical records. Extensive simulations and comparative analysis will be conducted to evaluate the framework's performance and efficacy to existing methodologies.

REVIEW OF LITERATURE

Many cryptographic methods have been proposed for use in IoT cloud systems to facilitate safe and accurate data transport. The primary goal of these endeavors has been to develop more robust and secure means of manipulating data. One innovative approach was employed in a research [14] to contract out to a fog layer the processes of signing, validating, and decrypting data collected from IoT devices. The length of the signature was significantly reduced and its independence from the number of linked characteristics was guaranteed by using this approach. There was still the computationally hard task of encryption on the Internet of Things side. To protect information from Internet of Things devices stored in the cloud, another study [3] offered an approach to access control based on CP-ABE (Cipher-Policy Attribute-Based Encryption). Here, a large chunk of partial CP-ABE decryption was executed by the cloud server using a user-specific transformation key. By closely associating identity features with the key holder, this key enabled authorized users to decode partly deciphered cipher text and recover data in plaintext. Other research have also investigated the integration of CP-ABE with cloud storage. To further ensure the safe retrieval of Internet of Things data stored in the cloud, one method proposed [15] used a CP-ABE-based storage strategy. This method decentralized decryption by storing public keys on the cloud and using an attribute authority management module to streamline the process. A recent effort [2] focused on data sharing in mobile cloud computing and outsourced the complete CP-ABE decryption procedure to a trusted proxy in the cloud. The user's involvement in decryption was reduced when a symmetric key was produced throughout the process. Nonetheless, external encryption was not the primary emphasis of this research. In the context of industrial IoT, a tag-aided encryption mechanism [16] has been proposed to safeguard item-level data during cloud-assisted IoT data transfers. Keys to participants' items allowed for the secure sharing of IoT records. Even while these methods usually did not have fine-grained access control to encrypted IoT data, some instances [17] [18] dealt with the security of data transfer and aggregation from IoT devices, especially in the healthcare sector.Recent initiatives have integrated blockchain with cloud computing to provide efficient platforms for data exchange and decentralized access management. A "blockchain" is a network of interconnected, immutable records stored in a sequential order of blocks that are both informational and time-stamped [8,9]. This technology serves as a digital ledger system for the purpose of maintaining records [10,11,12]. Data stored in each block is secure and impenetrable [10,11,12]. The decentralised nature of the blockchain makes all of its data publicly available. Public blockchains and private blockchains are the two main types of blockchains. Blockchains may be either public (also called permissionless) or private (sometimes called permissioned), with the former allowing access to everybody and the latter limiting it to registered users. Concerns that public blockchains cannot adequately protect the privacy and secrecy of sensitive health data are especially relevant to healthcare systems that are subject to privacy regulations such as HIPAA or GDPR [15].

EXISTING SYSTEM

• The authors have used a fog layer to handle the data signing, verification, and decryption for their Internet of Things (IoT) devices. Under this plan, their KPABS signature length remains fixed. Therefore, it does not rely on the quantity of signature qualities. But encryption, which is computationally intensive, is still handled entirely by the IoT. .

• The authors suggested a cloud-based access control system based on CP-ABE to protect data from the Internet of Things. Here, a user-specific transformation key is used to offload a substantial portion of the partial CP-ABE decryption phase from the cloud server. Because the identity qualities are connected to the key, the keyholder is

tightly related with the transformation key. Partial CP-ABE decryption allows authorized users to retrieve the plaintext from partly decrypted cipher text. .

• A CP-ABE-based storage model for secure cloud data storage and access was suggested by Xiong et al. for Internet of Things (IoT) applications. In order to reduce processing and storage overhead on a system level, this solution uses a cloud server to outsource decryption and stores public keys for both users and AAs in an attribute authority management module (AAM). .

• A plan to facilitate data sharing in mobile cloud computing was recently put forward by Sanchol et al. [2]. In this setup, the trustworthy proxy in the cloud is responsible for decrypting CP-ABE in its entirety. Through the calculation of the secret key, which is generated during decryption, the user is only able to decode the ciphertext using the symmetric key. But this piece of work didn't support using third-party encryption services.

• To safeguard item-level data for Internet of Things (IoT) records in a cloud-assisted industrial IoT setting, the authors suggested a tag-aided encryption method in. Participants in this system get item keys that enable secure communication during the transmission of the IoT record. .

Indeed, it is equally critical to aggregate health data acquired from IoT devices and to transmit it securely. Gathering raw data from different medical devices is the initial step before building and storing EMR data. A small number of studies have concentrated on the topic of pre-transmission encryption of IoT data. Nevertheless, they are unable to provide granular control over who may access encrypted IoT data.

In order to provide decentralized access control tasks like authentication, authorization, and accountability, as well as efficient data exchange, several recent studies have used blockchain technology in conjunction with cloud computing. As an example, Liu et al. [21] put out a privacy-preserving data sharing for EMRs that is based on blockchain technology. The plan calls for encrypting the EMRs using CP-ABE before storing them in the cloud. An immutable consortium blockchain stores the ciphertext index. But their CP-ABE decryption method isn't cut out for the Internet of Things cloud. .

• To provide granular authorization for IoT data, the writers presented the IoTChain paradigm in. This method encrypts the IoT stream before sending information to IPFS using attribute-based access control (A-BAC) and AES-128 encryption algorithms. Deploying smart contracts on the Ethereum blockchain also allows for encrypted keyword searches. But then the problem arises with symmetric key management.

• In their proposal, Zhang et al. put up a hierarchical data sharing framework (BHDSF) that is built on the blockchain. This framework would allow for quick retrieval of encrypted PHRs, fine-grained access control, and the use of CP-ABE and symmetric key encryption. For the purpose of shifting computing to the cloud, the strategy makes use of online/offline and outsourced CP-ABE decryption methods. The symmetric key in this technique is computed by the user using the search ciphertext and the intermediate ciphertext.

An Internet of Things (IoT) blockchain-based access control system for EHRs that relies on third-party encryption and decryption was suggested by S. Fugkeaw et al. One use case for smart contracts is the provision of user authentication checks. .

• The DSA-Block model, put out by Alshehri et al., is a blockchain-based system for dynamic secure access control. The technique used hyperelliptic curve cryptography (HECC) for user and device authentication in the IoT. A differential privacy technique was used to ensure the security of the IoT recordings prior to their storage in the cloud. .

• To ensure safe and efficient access to patient data, Cheikhrouhou et al. suggested a lightweight remote patient

monitoring system that is fog-enabled and built on the blockchain. A local chain would work in tandem with a fog node to take part in the consensus process; this would shorten the time it takes to retrieve data stored in the cloud, according to the suggested design. . A privacy-preserving method for safe misbehavior detection in lightweight IoMT devices was suggested by Ramadikha et al. in their publication. Using the Ethereum smart contract ecosystem, the authors enhanced data security by using privacy-preserving bidirectional long-short-term memory (BiLSTM).

DISADVANTAGES

• Since it enforces both encryption and access control, ciphertext-policy attribute-based encryption (CP-ABE) is not an appropriate option for outsourced data in the current system. .
• Ensuring that the secret key kept in inaccessible Internet of Things (IoT) devices or user terminals inside each medical department is protected from numerous users.

PROPOSED SYSTEM

In order to provide efficient, privacy-preserving, and lightweight EMR sharing based on the Internet of Things (IoT) with policy update capabilities, the system suggests a technique dubbed LightMED. The suggested system makes use of blockchain technology to facilitate auditing, decentralization of access control, and authentication. This requires encrypted data from the Internet of Things (IoT) and other treatment records to be securely aggregated for healthcare purposes. Additionally, we provide a signature technique that may be used to authenticate the source of data obtained from IoT devices, something that is currently lacking in most CP-ABE systems. By integrating with the cloud server and blockchain, a network of fog nodes may encrypt data using CP-ABE and reduce the computational and transmission costs associated with data outsourcing. We suggested an attribute tree-based encryption to protect the privacy of the access policy when it is sent from the data owner to the fog node, so that the fog nodes may encrypt the data without disclosing its content. We enhance the secret key calculation method from [2] for the decryption segment by dividing the random components used to calculate the key. Because of this enhancement, our technique may greatly lower the cost of re-encryption conducted by the fog nodes and does not need the end user's device to keep the secret key.

ADVANTAGES

1. Our suggested approach, LightMED, offers fog node environments both outsourced encryption and decryption that is lightweight. With the help of the aided fog node, this strategy suggests a novel method of dual encryption that combines the Advanced Encryption Standard (AES-256) and Ciphertext-Policy Attribute-based-Encryption (CP-ABE) into a very lightweight algorithm, allowing the outsourcing of cryptographic processing costs to and from the cloud. .
2. The end user's device is not necessary to store the secret key according to our suggested system. Key leakage issues are prevented by this. .
3. In order to facilitate effective policy update management for EMRs that are outsourced, we developed a lightweight algorithm. Our system's data owners may make policy updates without worrying about the expense

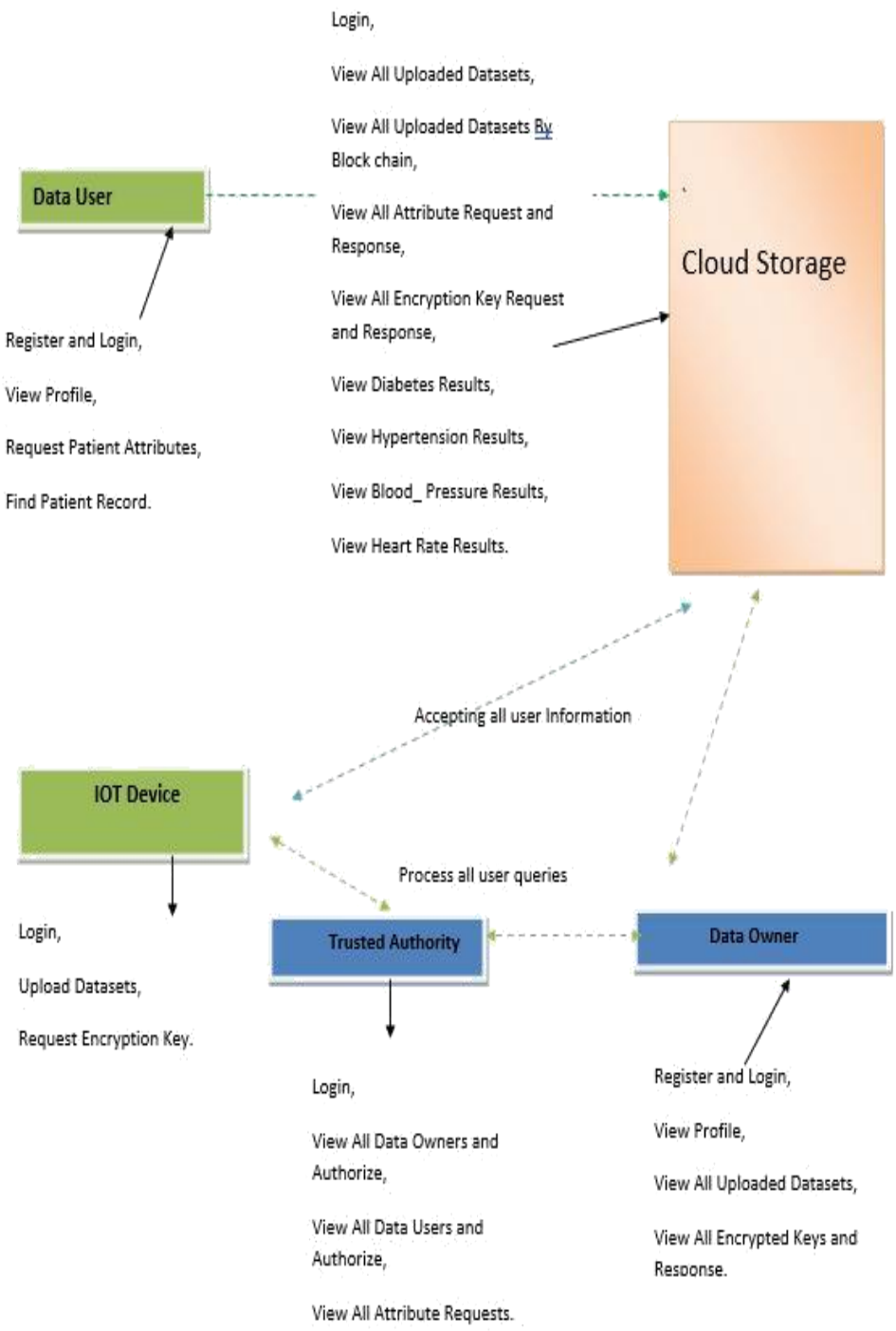
of re-encrypting cipher text since the fog node handles it. .

4. We presented a lightweight and safe technique for encrypting data sent by IoT devices and another for decrypting it after it has been received. Before creating EMRs using our lightweight encryption and digital signature, we also implemented a secure Internet of Things data aggregation with source authentication. After a sensor has collected data and sent it to an aggregation terminal, these two algorithms may stop any information about the patient from leaking. .

5. To allow efficient ciphertext decoding, we used blockchain technology to store certain cryptographic parameters, create ciphertext indexing, and provide decentralized access control and authentication. In order to facilitate ciphertext indexing and decryption, we combined the encrypted symmetric key's ciphertext with the encrypted patient's data. All transaction records are maintained in an immutable way on the blockchain, and we have established a set of smart contracts to automate the algorithms flexibly to support these activities.

6. To back up the efficacy of our plan, we conducted trials and comparison analyses. To prove that our suggested strategy was better than previous studies in the field, we compared it to previously published articles.

SYSTEM ARCHITECTURE



MODULES

Individual Using Data Data users may access features including profile viewing, attribute requests, and record retrieval in this module. . Internet of Things Tool He enters his credentials (username and password) to access this section. Login, Upload Datasets, and Request Encryption Key are some of the tasks that the recipient may do after logging in.

Owner of Data The following operations are available to the sector in this module: Sign up and log in, check out the profile, see all the datasets that have been uploaded, see all the encrypted keys, and read the response. Respected Expert The following operations are available to the sector in this module: Once logged in, you will be able to see all owner and authorize requests for data, as well as all user and attribute requests.

Data Storage in the Cloud. . On top of managing a server to store data, the cloud also allows users to perform things like log in and see all uploaded datasets. In the blockchain technology Please review all of the requests and responses about attributes and encryption keys. Keep an eye on your blood sugar, blood pressure, heart rate, and hypertension readings.

CONCLUSION

In order to provide outsourced IOT-EMRs safe, granular, and lightweight access control with fog computing and blockchain, we have presented the Light MED scheme. Secure aggregation and encryption of IoT data were suggested in our system. Full outsourcing of CP-ABE encryption with privacy preserving policy and decryption to fog nodes helps minimize total communication and computation costs for data owner and end-user, allowing for fine-grained and lightweight data access. We used blockchain technology to provide audits, secret random parameter storage, data indexing, and decentralized authentication. In addition, we suggested a simple technique for updating policies in the IoT cloud to facilitate policy development. In the end, we ran the tests, and the results proved that our suggested cryptographic operations perform much better than the comparable works. What's more, our system's throughput proved that our scheme is efficient and scalable enough for actual deployment. Still, we will be focusing our future efforts on enhancing the handling of user and attribute revocation, which is an important area that has not been well addressed. Another remaining concern is value-guessing attacks on characteristics. Our innovative Policy Tree Encryption technique has partly addressed this issue. But this doesn't solve the whole problem since it doesn't protect the cipher text's visibility of attributes. Thanks to the foundation we've laid, we're optimistic about the future and can't wait to keep refining the scheme to reveal hidden qualities. In conclusion, our system's capabilities may be enhanced by fully using Fog Computing. This is because of the idea of intelligent resource sharing, which involves dynamically offloading identical or almost identical processes to adjacent fog nodes based on their properties. Our system's performance will be much enhanced by implementing this idea.

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,’’ *IEEETrans. Cloud Comput.*, vol. 10, no. 2, pp. 1008–1020, Apr. 2022, doi: 10.1109/TCC.2020.2985046.

[4] J. Lai, R. H. Deng, C. Guan, and J.Weng, ‘‘Attribute-based encryption with verifiable outsourced decryption,’’ *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[5] S. Lin, R. Zhang, H. Ma, and M.Wang, ‘‘Revisiting attribute-based encryption with verifiable outsourced decryption,’’ *IEEE Trans. Inf. ForensicsSecurity*, vol. 10, no. 10, pp. 2119–2130, Oct. 2015.

[6] S. Abdollahi, J. Mohajeri, and M. Salmasizadeh, ‘‘Highly efficient and revocable CP-ABE with outsourcing decryption for IoT,’’ in *Proc. 18thInt. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, Sep. 2021, pp. 81–88, doi: 10.1109/ISCISC53448.2021.9720469.

[7] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, ‘‘Multi-authority ciphertext-policy attribute-based encryption with accountability,’’ in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur.*, Mar. 2011, pp. 386–390.

[8] Z. Liu, Z. Cao, and D. S. Wong, ‘‘Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay,’’ in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2013, pp. 475–486.

[9] Z. Liu and D. S. Wong, ‘‘Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable,’’ in *Informationand Communications Security* (Lecture Notes in Computer Science), vol. 9543, S. Qing, E. Okamoto, K. Kim, and D. Liu, Eds. Cham, Switzerland: Springer, 2016, pp. 109–124.

[10] S. Fugkeaw, ‘‘A lightweight policy update scheme for outsourced personal health records sharing,’’ *IEEE Access*, vol. 9, pp. 54862–54871, 2021, doi: 10.1109/ACCESS.2021.3071150.