RESEARCH ARTICLE **SPECIAL ISSUE**

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05, Issue 05S May
www.rspsciencehub.com

Check for updates

http://dx.doi.org/10.47392/irjash.2023.S065

International Conference on intelligent COMPUting TEchnologies and Research (i-COMPUTER) 2023

ABAC Scheme on Electronic Health Records Using Hyperledger Fabric

Ashwin Rupak S A B [1], Janarthanan J [1], Kishore Kumar N [1], Harissh S [1], Sasi Kumar R [2]

[1]Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science and Engineering, K. Ramakrishnan College of Engineering, Tamil Nadu, India

Email: ashwinhiro01@gmail.com

Article History

Received: 26 February 2023
Accepted: 21 March 2023

***Keywords**:*

Attribute Based Access Control (ABAC);
Hyperledger Fabric;
Electronic Health Record (EHR);
Rivest Shamir Adleman (RSA);
Patient records;
Interplanetary File System (IPFS))

Abstract

In this modern world, data is getting more significant with new emerging technologies, and a transparent system must be made with security mechanisms. For example, an Electronic Health Record (EHR) is a system that records patient data in a digital format across different healthcare settings. The ultimate benefits of Blockchain technology are to safeguard patient records and pave a path for health centers, clinics, and medicals. A high-level invulnerable system is required to prevent the rising cybersecurity threats targeting these organizations. A Blockchain that fulfills the HIPAA regulation is a protective barrier and transparency required by many fields. Attribute-based access control (ABAC) is a scheme that provides an effective authentication and authorization model that considers attributes from the user, instead of roles, to grant permission to the user to access. This system makes it easier for Certificate Authorities (CA) to manage user permissions by assigning specific rights and privileges based on the individual's characteristics. Thus, writing policies will secure data transparency as the one requested can only view the data if they satisfy the policy's criteria.

1. Introduction

More cyberattacks are now focusing on medical records, and there is a lot of data currently being produced because of these technologies, such as the Internet of Things (exchanging of information over other devices) and big data (consists of large, complex, difficult data which cannot be handled with ease) rapid development. (Liang et al.) Information about patients must be protected at all costs in medical facilities. The laws that are in place in the United States are particularly severe whenever it falls to the safeguarding of information of patients. A medical facility may face severe consequences for information loss. (Kumar, Palanisamy, and Sural) If an attack happens on a pharmacy or hospital and the information is stolen, the knowledge of patients and their lives are at risk (for example, identity theft). Patients' personal information breaches can result in expensive fines for organizations. (M. Joshi, K. Joshi, and Finin) Because so much of this data is in transit and hence susceptible, it is incredibly challenging to secure. The value of these resources must be explored appropriately to ensure that all parties can share them safely. People are worried about two main issues related to this process: their private information or company secrets and how safe the data will stay when stored in the cloud. Cloud storage offers many benefits, like on-demand payment, load balancing, elastic expansion, simple management, etc. Increasingly consumers

opt to use the cloud for storing their data; however, even while cloud storage offers some user convenience and addresses the data problem. (M. Joshi, K. P. Joshi, and Finin)

Centralized, island-style storage system also requires the data owner to have complete faith in the third party for cloud service providers to take the position of people or businesses in exercising control over the data. There isn't a third party that can be entirely trusted. They might sell user information with malice, motivated by personal interests; they might attack a data center with malicious intent from outside and might experience internal issues with the cloud platform system that could result in the disclosure and loss of the user's information. (Wu et al.) Moreover, they might not be able to guarantee the accuracy of their data. Hence, it has become urgently necessary to find a solution to the point of failure brought on by centralized data storage and hostile internal and external attacks and protect the data integrity. (Li et al.)

People's attention is also focused on how to safely share data among numerous parties, which entails the data access issue, or who has access to a user's personal data, the data they can get into, and the operations they can be performed on those data. In some instances, identity authentication, access control, and other methods restrict others' access to user details. (Y. Wang et al.)

However, the formal identity identification and access control are typically handled by a central organization, this data control remains with corresponding third parties, which are not entirely trustable, and the specifics of user data usage are still ambiguous. Satoshi presented a distributed ledger system (blockchain) without the requirement to record transactions from a reliable third party between two parties in 2008. (Jayanthilladevi, Sangeetha, and Balamurugan) Every transaction on it is immutable, traceable, and non-repudiable. To assure data integrity, give users access such that the history of the operation can be audited, and eliminate process transparency, some researchers proposed combining cloud storage with blockchain technology. They suggested encrypting data before storing it in the cloud and proof of storing over data integrity verification on the blockchain. (Hidayah and Ramli)

1.1. Tight access regulations:

Use member service providers to establish and control user access regulations and associated permits. A user must be authorized before they may join the fabric. For the convenience of developers, support for developing smart contracts in popular languages such as Java, Go, Node, and others is offered.

1.2. General programming language:

For the convenience of developers, support for developing smart contracts in widely used languages like Java, Go, Node, and others is offered.

1.3. Get rid of mining incentives and miners:

Use the new execute-order validate transactional method. The transaction is first tested to check that it is correct by the endorsement node. The pluggable consensus protocol classifies it and is ultimately confirmed in line with the present endorsement strategy. Due to the concurrent execution of transactions and the fact that only a few nodes are subject to the system endorsement policy, it provides excellent performance and network scalability.

1.4. High-performance storage systems:

Different chain codes' world states are inaccessible to one another. The term "world state" refers to the account status over time. Second, it is compatible with various database management systems, including CouchDB and Go Level DB.

2. Related Work

Health Centres and other medical services are increasingly becoming targets of terrorist attacks worldwide. Patient data is highly confidential. Hospitals cannot function without information and may be forced to close. The HIPAA law protects patient information in the United States. (Hidayah and Ramli)

According to the United States, HIPAA was implemented in 1996. In August 2002, the Privacy Regulation linked with it was amended and ready for adoption. The purpose of this new rule was intended to provide individuals with more control over their data and to make medical facilities liable for data breaches. If a hospital or medical facility is compromised, they may face significant fines. (Deleon, Choi, and Ryoo)

The data will be stored inside the Interplanetary File System (IPFS), a protocol, and a peer-to-peer

network for storing and sharing data in a centralized file system. However, the data passed onto the Interplanetary File System (IPFS) are vulnerable to attack, and data get stolen because of the insecurity. (Hao et al.)

Most research focuses on two primary areas to address the privacy leakage issues brought on by centralized cloud storage:

Access control and encryption ensure data confidentiality while preventing illegal access.

As for encryption standards, it is required to encrypt data before sending or processing it. For that, an encryption algorithm has been used to safeguard the data and prevent being hacked by attackers. In encryption standards, there are two encryptions: symmetric encryption and asymmetric encryption.

Symmetric encryption uses a single key to encrypt and decrypt data. So that it becomes vulnerable once the key has been found and there is a possibility of the key being found. In this situation to assess, an asymmetric algorithm will be used to encrypt and decrypt the data, where different keys have been used for encryption and decryption.

Here, an algorithm was developed by these cryptologists Rivest, Shamir, and Adleman and named after the algorithm from the first letter of their name called RSA. This algorithm uses a different key to encrypt and decrypt the data. However, it holds a shared secret key, so it isn't easy to decrypt the data inside the encrypted one because of factoring over large integers. (Guo et al.)

Then is the access control technique, which can access the requested resource for several available schemes such as Role-Based Access Control Scheme (RBAC) and Attribute-Based Access Control Scheme (ABAC). A role-Based Access Control Scheme (RBAC) is a technique of limiting network access established on individual roles of users within an organization. It ensures that employees have only the information they need to do their jobs and that they do not have access to irrelevant information. (S. Wang et al.)

But the problem with Role-Based Access Control Scheme (RBAC) is that role explosion, as the new roles have been created, makes it confusing and may cause vulnerability to access the information. The other problem is that it is difficult and expensive to implement. Therefore, migrating to Role-Based Access Control Scheme (RBAC) might face unforeseen challenges. (Kakei et al.)

To overcome this problem, static authorization's shortcomings are efficiently fixed by Attribute-Based Access Control Scheme (ABAC). Moreover, it is a versatile access control mechanism since it grants users access rights under qualities and supports complicated contexts. (Benhamouda, S. Halevi, and T. Halevi)

3. Technologies Used

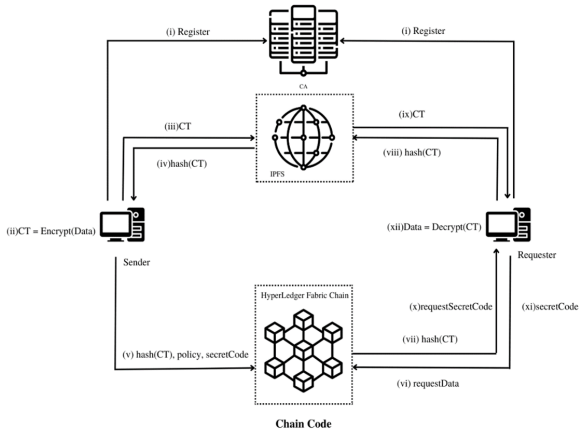

FIGURE 1. Proposed System Architecture

3.1. Hyperledger Fabric

Fabric, a permission, modular blockchain, enables programming and execution in mainstream languages. Typical fabric core parts include:

3.1.1. Management of Identity:

Hyper Ledger Fabric offers Member Service Provider (MSP) service. It oversees managing and verifying each node in the network, including clients, peers, and orders. In addition, Fabric-CA leads provide certificates to the users and sign their private keys for network nodes as a particular implementation of Member Service Provider (MSP). The node has to be trusted by the authority that provides certificates to verify the identity, and the Member Service Provider (MSP) provides services for registering the node in the blockchain. Without the permission of the certificate authority, the node cannot permit to do the registration process by the Member Service Provider (MSP).

3.1.2. Transaction management :

This primarily entails installing nodes with chain codes. The endorsing node must approve a transaction. This indicates that the endorsement node executes the relevant function under the chain code placed on it before obtaining the relevant endorsement result.

3.1.3. Accounting management:

The transaction log and world status are the two sections of Fabric's ledger. The ledger is identical between nodes connected to the same channel. After a transaction is completed, the world state captures the most current state of all its keys, and its transaction log contains a block-by-block history of all trades.

3.2. Attribute-based access control

The four essential components of attribute-based access control (ABAC) are as follows: The components are connected by this attribute to build up a strategy that creates invulnerability and flexibility to act for the features that information is preserved and used by the right hands. Some of these elements are subject (who acted to gain access), object (where the operation took place), operation (the action the subject wanted to do), and environment (constraints of factors of real-time). It is better suited for well-tuned access control in complex situations because attributes can be used to reflect roles and authorization in the access control process. The benefits of attribute-based access control techniques are as follows:

- Fine-grained approval Attributes and access control place restrictions on entities. Attributes limit entities, and access policies can be established as highly flexible. For example, it can identify whether an attribute matches a regular expression, and logic AND or logic OR can be used to build various access rules.
- Independent authorization: Data owners can create access policies and offer policy interfaces. Policies don't need to be handled by administrators. Identity division, for instance, is no longer carried out by specialized entities such as identity-based access control.
- It is simple to control the attributes: Several real-world data, such as organization position, address, etc., can be used as attributes. In the Internet of Things, resources have several common attributes, such as device IP address and ID. One-to-many relationships make establishing connection between the subject and the object simple.
- Access control is inexpensive since it may be dynamically changed to consider the current circumstances. In a medical setting, for example, if a nurse oversees a patient, the admin only must create an access policy and enter the word "grant access." After the patient has been sent out, only the admin has the authority to remove this policy. Only one class of roles' permissions may be specified via role-based access control, which does not provide well-cleared control over a user's access authorization.

4. System Architecture

As the proposed system contains three modules based on the HIPAA-Compliant, as it satisfies the first module from the First Rule of HIPAA, The Security Rule, a security mechanism is implemented to protect the information by encrypting it using the RSA algorithm. Then the second module is composed of the Second Rule of HIPAA, The Privacy Rule, which is implemented with the help of the Attribute Based Access Control Scheme (ABAC). Finally, the third module comprises the Third Rule of HIPAA, The Breach Notification, implemented with Blockchain's help.

- The sender registers themselves to get the Identity and private key with the help of the RSA algorithm and the certificate from the authority.
- The Sender encrypts his plain data into cipher text as the data being protected by encrypted using their public key.
- The Cipher Text sends to the IPFS by the sender. The data has been stored on the IPFS.
- The IPFS resends a hashed value of cipher text hash (CT) by passing the cipher text to the hashing function that the ciphered data stored on IPFS while the hashed value is transmitted locally.

- The hash (CT), secret Code sent along with the specified policy by the sender to make it available only to those who match the criteria.
- The requester requests the data from the Hyperledger fabric once registered and certified by the certified authority.
- The requested data's hash (CT) is only sent if the policy matches the requester's identity.
- The hash (CT) has been sent locally to the requester system and then retransmitted to the IPFS.
- The IPFS been sent back to the Cipher Text to the requester respective to the hash (CT).
- The requester must know the secret code to decrypt the text. Hence a request has been sent to request a secret code (request Secret Code) to get the secret code.
- The secret code has been sent to the requester to decrypt the cipher text.
- The requester decrypts the cipher text with the private key and secret code to get the data. With the help of the ABAC scheme, it prevents the attacks happening on blockchain, as it was explained in next section.

5. Security Analysis on Attacks

5.1. Phishing Attacks:

This attack involves taking over the user's credentials by sending an email from a legitimate source to get hands on the user's credentials.

However, the access in ABAC considers the device's attributes and other factors to gain access, so it is impossible.

5.2. Routing Attacks:

While the data is encrypted with the help of the RSA algorithm unless knowing the sender or receiver's private key, it is difficult to decrypt the data.

However, before that, the user has to be valid as he owns a certificate from the authority to begin communicating with it.

TABLE 1. Sample Table format

S. No	Attacks	Prevention
1.	Phishing Attack	Implemented through Attribute Based Access Control scheme
2.	Routing Attack	With the help of RSA algorithm implementation.
3.	51% Attack	It can't be possible to happen.
4.	Brute Force Attack	With the help of RSA algorithm implementation.
5.	Sybil Attack	Implemented through Attribute Based Access Control scheme

5.3. 51% Attack:

In this attack, a group of miners tends to gain resources if they can get more than 50%, which is required to manipulate the ledger.

However, In Hyperledger fabric, 51% of attacks can't possibly happen.

5.4. Brute Force Attack:

As a brute force, a trial-and-error method to try different possible passphrases to get into the network and get access to it. It can be prevented by RSA algorithm implementation.

5.5. Sybil Attack:

In this attack, one will try to conquer the surrounding nodes to gain the transaction of the peer node to get the information. It can be prevented with the help of the Attribute Based Access Control Scheme

6. Results and Analysis

From the experimental result analysis, we learned that the proposed model significantly improves between transactions over peers as it is stable over the given dataset. Furthermore, the information is requested, and access is provided to peers who can manipulate it only if they meet the policy criteria and have frequent transactions as quickly as possible.

Figure 3 depicts the throughput of average latency; as the transaction is stable, throughput is controlled across the latency such that the system

shows the performance quality for the proposed system.

This involves that the patient records can be retrieved and there won't be any intervention between delay rate because of network traffic. As the peer gets the access, can get the data from the transaction and manipulate it based on the policy that sender created.

Figure 2 shows that the send rate across throughput shows relatively good results and that the scheme and encryption algorithm for privacy doesn't affect majorly over the transactions as it keeps the flow of transactions within the network and gets the designated result.

Thus, by that, the researchers concluded that using the proposed system relatively met the standards for the transaction without delaying or meeting the rate of failure as it is tested in experimental analysis.

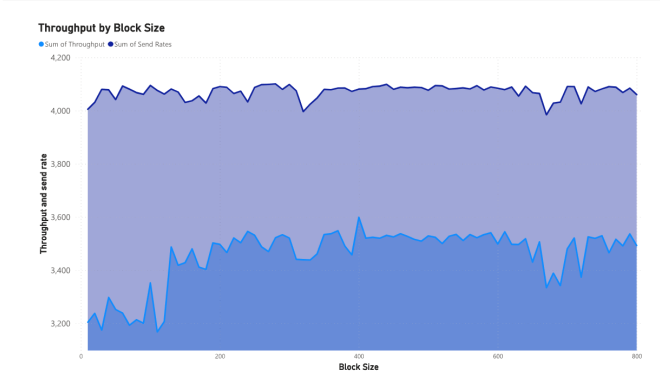

FIGURE 2. Throughput by Block Size

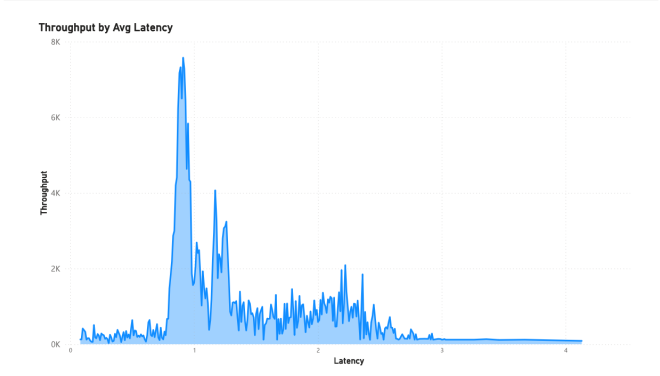

FIGURE 3. Throughput by Average Latency

The proposed model system provides stable management over electronic health records by following the reliant HIPAA-compliant, which helps to be invulnerable to attacks and maintains transparency of information of patients. First, the Security Rule paves the path for data to be passed secretly between the sender and requester while it remains unknown to others with the help of the RSA algorithm because of its secret shared vital feature. Then, The Privacy Rule allows up a scheme called ABAC to make it available, which satisfies the criteria, as the requirements consider subject, object, environmental conditions, policy, and operation to define the access to be given or rejected it. And then, The Breach Notification Rule, as the blockchain of Hyperledger is private, breaching should be possible if the data is taken over 51% unless it can't be. So that makes the system to be invulnerable to most attacks.

7. Future Scope

However, the proposed solution isn't tested in real-time, and unknown about its performance is on an objective basis.

Future work must be done to check the performance in the real-time scenario to make it available for real-time use.

References

Benhamouda, F, S Halevi, and T Halevi. "Supporting private data on Hyperledger Fabric with secure multiparty computation". *IBM Journal of Research and Development* 63.2/3 (2019): 3:1–3:8.

Deleon, Colin, Young Choi, and Jungwoo Ryoo. "Blockchain and the Protection of Patient Information: Using Blockchain to Protect the Information of Patients in Line with HIPAA (Work-in-Progress)". *2018 International Conference on Software Security and Assurance (ICSSA)* (2018): 34–37.

Guo, Hao, et al. "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-based Cryptographic Mechanisms". *IEEE Transactions on Network and Service Management* (2022): 1–1.

Hao, Guo, et al. "Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture". *2019 IEEE International Conference on Blockchain (Blockchain)* (2019): 44–51.

Hidayah and Kalamullah Ramli. "HIPAA-based Analysis on the Awareness Level of Medical Per-

sonnel in Indonesia to Secure Electronic Protected Health Information (ePHI)". *2021 IEEE International Conference on Health, Instrumentation & Measurement, and Natural Sciences (InHeNce)* (2021): 1–6.

Jayanthilladevi, A, K Sangeetha, and E Balamurugan. "Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy". *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (2020): 244–247.

Joshi, Maithilee, Karuna P Joshi, and Tim Finin. "Delegated Authorization Framework for EHR Services Using Attribute-Based Encryption". *IEEE Transactions on Services Computing* 14.6 (2021): 1612–1623.

Joshi, Maithilee, Karuna Joshi, and Tim Finin. "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems". *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (2018): 932–935.

Kakei, Shohei, et al. "Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric". *IEEE Access* 8 (2020): 135742–135757.

Kumar, Ritik, Balaji Palanisamy, and Shamik Sural. "BEAAS: Blockchain Enabled Attribute-Based Access Control as a Service". *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2021): 1–3.

Li, Fengqi, et al. "EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem". *IEEE Transactions on Services Computing* (2021).

Liang, Xiao, et al. "A Blockchain and ABAC Based Data Access Control Scheme in Smart Grid". *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)* (2022): 52–55.

Wang, Shuai, et al. "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends". *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49.11 (2019): 2266–2277.

Wang, Yong, et al. "Cloud-Assisted EHR Sharing With Security and Privacy Preservation via Consortium Blockchain". *IEEE Access* 7 (2019): 136704–136719.

Wu, Huanyu, et al. "MB-EHR: A Multilayer Blockchain-based EHR". *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2021): 1–3.

Embargo period: The article has no embargo period.

To cite this Article: , Ashwin Rupak S A B, Janarthanan J , Kishore Kumar N , Harissh S , and Sasi Kumar R . "**ABAC Scheme on Electronic Health Records Using Hyperledger Fabric**." International Research Journal on Advanced Science Hub 05.05S May (2023): 489–495. http://dx.doi.org/10.47392/irjash.2023.S065