IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Review of transfer of Secret Data Using Re-Encryption Technique with Hyperledger Fabric Based on Blockchain

Bhagyashri H. Adhau[1],Prof. S.B.Rathod[2]

*Department Of Computer Science and Engineering, Sipna COET*

**Abstract—** Providing a consistent distributed ledger, shared by a set of "peers." As with every blockchain architecture, the core principle of Hyperledger Fabric is that all the peers must have the same view of the shared ledger, making it challenging to support private data for the different peers. Extending Hyperledger Fabric to support private data (that can influence transactions) would open the door to many exciting new applications, in areas from healthcare to commerce, insurance, finance, and more.

Personal health record system (PHR system) stores health-related information of an individual. PHR system allows the data owner to manage and share his/her data with selected individuals. Blockchain technology becomes a potential solution due to its immutability and irreversibility properties. Unfortunately, some technical impediments such as limited storage, privacy concern, consent irrevocability, inefficient performance, and energy consumption exist. This work aims to handle these blockchain drawbacks and propose a blockchain-based PHR model. The proposed model is built using the blockchain technology to support a tamper resistance feature. Proxy re-encryption and other cryptographic techniques are employed to preserve privacy. Features of the proposed model include fine-grained and flexible access control, revocability of consent, auditability, and tamper resistance. A detailed security analysis shows that the proposed model is provably secure for privacy and tamper resistance. The performance analysis shows that the proposed model achieves a better overall performance compared with the existing approach in the literature thus the proposed model is more suitable for the PHR system usag.

***Keywords: Private Blockchain ,Hyperledger Fabric,Re-Encryption.***

## I. INTRODUCTION

A blockchain is a distributed system for recording history of transactions on a shared ledger, providing consistency (i.e., all participants have the same view of the ledger) and immutability (i.e., once something is accepted to the ledger, it cannot change). First popularized for crypto-currencies such as Bitcoin, blockchain technology today is gaining momentum in other areas as well, and is touted by some as a disruptive change akin to open-source software or even the Internet.

Hyperledger is an open sourced community of communities to benefit an ecosystem of Hyperledger based solution providers and users focused on blockchain related use cases that will work across variety of industrial sectors. Hyperledger believe that every business and industries is unique in it's way and the application that they using must be personalized in its own way unlike Ethereum Blockchain that runs on a very generalized protocol that everything runs on its network.

The Hyperledger Fabric is a permissioned blockchain, where writing to the ledger requires some credentials. The participants that are allowed to write to the ledger in Hyperledger Fabric are called peers (and typically there are only a few of them). This setting makes it easier to control the transaction on the ledger, and is typically faster than public blockchains that are used in most crypto-currencies. Nearly all blockchain architectures support the notion of smart contracts,

## II. BACKGROUND

### 2.1 Background History

In healthcare, we have large volumes of data coming in from EMRs. Most of that data is collected for recreational purposes according to Brent James, of Intermountain Healthcare [4]. But neither the volume nor the velocity of data in healthcare is truly high enough to require for suggesting proper healthcare prescriptions. The work done with health systems shows that only a small fraction of work is done that serves irrelevant to the current practice of medicine and its corresponding analytics use cases. So, the vast majority of the data collection in healthcare today could be considered recreational. Although that data may have value down the road as the number of use cases expands, there aren't many real use cases for much of that data today. But as the data mining and security techniques are growing on increasing it is necessary to develop for the getting useful results.

### 2.2 Existing System

Most of the time, for critical diseases physicians have an imperfect knowledge of how they solve diagnostic problems. Then the first operational Bayesian CDSS for the diagnosis of congenital heart diseases is developed based on history, physical exam, and cardiac catheterization findings [5]. After that Schurink, discussed computer-based decision-support systems to assist Intensive Care Unit (ICU) physicians in the management of infectious diseases. As the privacy of the patient's information becomes more and more important, naive Bayesian classification were considered as a challenge to privacy-preservation due to their natural tendency to use sensitive information about individuals.

The data in the existing privacy-preserving naive Bayesian classifier scheme were distributed and stored in different parties as horizontal and vertical partitioned manner as a part of the whole data space. One party should manage and store these data as plaintext. But, along with the development of cloud computing technique, outsourcing the encrypted data to cloud server to store was more common. However, cloud server was always a third-party server. Storing the patient health data in the third-party servers caused serious threats to data privacy. So it was imperative for user to store and manage the healthcare data in a privacy-preserving way.

## III. LITERATURE REVIEW

Putting private data on the ledger comes with an inherent dilemma: If everyone sees the same ledger, how can we have private data that some can see but others cannot? A common solution in many systems is to put on the ledger only an encryption (or a hash) of the private data, while keeping the data itself under the control of the party that owns it. Of course, this solution on its own is not enough if the smart contracts depend in any way on the private data (as in the use-cases above). Several existing systems offer partial solutions.

-Balaji Prabhu, et.al.has also worked on making the trading system of agriculture more transparent from farmer to consumer by avoiding the middleman.

-Abdelali El Bouchti, Houssine Bouayad and Youness Tribis proposed a Paper on A Systematic Mapping Study of Management of Supply Chain using Blockchain. Their effort was aims to analyze and explore the state-of the-art on the BlockChain Technology applications for Supply Chain Management. They have tried to identify the gaps available in SCMs by blending the existing and available evidence.

Tara Salman, Maede Zolanvari et.al have discussed about possible Security Services Using Blockchains.

HYPERLEDGER FABRIC CHANNELS. Hyperledger Fabric implements channels, which are essentially separate ledgers. The data on a channel is only visible to the members of that channels, but not to other peers in the system. This solution provides some measure of privacy (from non-member peers), but it still requires that all members of a channel trust each other with all the data on this channel.

USING ZERO-KNOWLEDGE PROOFS. Zero-Knowledge proofs (ZKP) allow a prover to convince others that a certain statement is true, without revealing any additional information.

Using ZKPs is enough when the smart contract depends on the private data of a single participant: The party who knows the secret can run the smart contract on its own, and then prove to everyone else that it did so correctly. For example, in a setting where participants have accounts with secret balance on the ledger, a participant wishing to buy a $100-item can use ZKP to prove that its balance is greater than $100. One examples of this approach is the Zcash currency, that supports a very general form of ZKPs.

However, ZKPs are not sufficient in settings where the smart contract depends on the secret information of more than one participant. For example, if we have one user with secret balance and another with secret reserve price

for an item, ZKPs on their own are not enough for checking if the balance of the first user is bigger than the reserve price of the second. (Indeed ZKPs are not sufficient for any of the use cases that we sketched before.)

ENIGMA. The Enigma system, uses secure-MPC protocols to implement support for private data on a blockchain architecture. The main difference between our solution and Enigma is that we integrate secure-MPC protocols within the blockchain architecture itself, while Enigma uses off-chain computation for that purpose. here we just note that on-chain computation seems like a better match for a permissioned blockchain such as Hyperledger Fabric.

## IV. EXISTING METHODOLOGIES

The performance depends on which technique use, amount of data required by technique, time and complexity parameters. Many method are proposed for object tracking and detection.

**Table 1: Performance of Existing Methods**

| Paper Title | Authors | Year of Publishing | Methods Used | Limitations |
|---|---|---|---|---|
| Computer assisted decision support for the diagnosis and treatment of infectious diseases in intensive care units, | C. Schurink, P. Lucas, I. Hoepelman, and M. Bonten | 2005 | Computer Assisted Clinical Decision Support System (CDSS) | It faces challenge to privacy-preservation due to their natural tendency to use Sensitive information about individuals. |
| Heart Disease Prediction System using Naive Bayes | Dhanashree S. Medhekar, Mayur P. Bote, Shruti D. Deshmukh | 2013 | 1. Categories medical data into five categories namely no, low, average, high and very high.<br>2. Naive Bayes algorithm is based on Bayesian Theorem is used and classification (training) and prediction (testing) will be performed. | 1. The system is only work for Heart diseases only.<br>2. Accuracy of the system is not always same and vary on algorithm and database used. |
| e-Health Cloud: Privacy Concerns and Mitigation Strategies | *Assad Abbas, Samee U. Khan* | 2015 | 1. digital signature and certificates based authentication<br>2. Different kinds of encryption techniques | 1. Outsourcing the sensitive health information to the third-party cloud providers can result in serious privacy concerns.<br>2. Applying number of Cryptographic techniques makes it time consuming |
| Heart Disease Prediction System | V. Krishnaiah, | 2016 | 1. Fuzzy K-NN classifier<br>2. Fuzzy Data mining techniques | 1. Success rate depends upon the parameters consider |

| | | | | |
|---|---|---|---|---|
| using Data Mining Techniques and Intelligent Fuzzy Approach: A Review | G. Narsimha, N. Subhash Chandra | | | 2. Accuracy depends on tools used for implementation |

## V. PROPOSED METHODOLOGIES

The Blockchain business solution is implemented by providing a connection between its individual organizations, for storage and exchange of information, as well as for its processing. The data are visible only between the organizations that have access rights, for which channels of communication have been established between them. To maintain the correctness of the data during recording and storage, peers are configured within the organization to maintain the operability of the network.

***peers' role and the consensus algorithm***

The Hyperledger Fabric ledger consists of two distinct parts: world state and blockchain. The first is a database that maintains a cache of the current values of the attributes of an object represented by key-value pairs. The exploitation of the world state allows programs to directly access the value of an object without having to traverse the entire blockchain to calculate it. The second is the blockchain transaction log which stores all the changes that led to the current value in the world state collected in blocks hung one in the other to form a chain.

In Hyperledger Fabric, each peer keeps a copy of the ledger (world state + blockchain) and the update of the copy is carried out by the peers individually through the consensus algorithm. It ensures that every peer will do the same update and that they will, therefore, have identical copies of the ledger.

Hyperledger Fabric network consists of a set of peers which can assume three distinct roles.

• *Endorser* which receives and executes transactions (transaction proposal) coming from client applications.

It is the only type of peer on which a Chaincode must be installed and is, therefore, the only one that performs it. They execute the request and reply sending back to the client an endorsed result (endorsed transaction proposal).

• *Orderer* is the peer that deals with creating transaction blocks. It receives endorsed transaction proposals and inserts them in a block together with others in an orderly manner.

• *Committer* which checks the validity of all transactions individually contained in the received block and applies the block to the ledger. All peers take on this role.

***Proxy Re encryption Scheme.*** The proxy re encryption scheme is an asymmetric cryptosystem that enables its users to share their decryption capabilities with others. Under the proxy re encryption scheme, the ciphertext—encrypted with the user public key—can be reconstructed in such a way that another user can decrypt it by using his/her private key although the ciphertext is not originally encrypted with his/her public key. the data will not be fully decrypted during the transmission. thus, the scheme will be a useful method to create a secure data sharing scheme. To share the data under the proxy re-encryption scheme, the data owner must send the re-encryption key to the proxy. However, the proxy will not be able to gain any information on the original data from there-encryption key. The re-encryption key is generated from the combination of the owner's secret key and the intended-user's public key. thus, the proxy re-encryption scheme is flexible to create an access control management system in our proposed model.

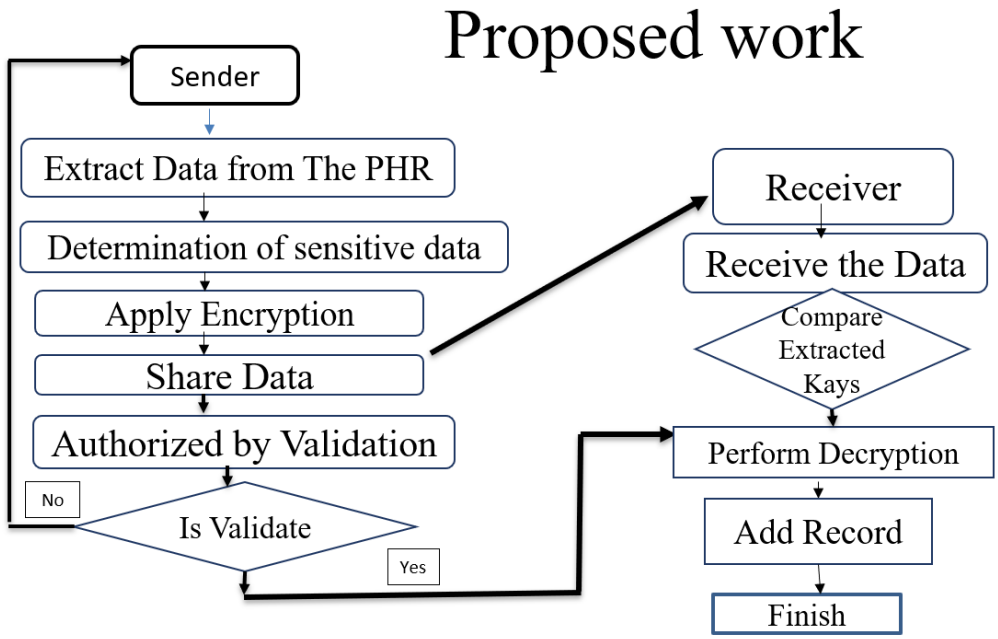


**Figure 1: Block diagram of Proposed Methodology**

**OBJECTIVE:**

- Unauthorized user can't get access to the data.
- Authorized user can easily modify, upload, and share their data.
- Owner apply security without retrieving the entire copy of data.
- It does not reveal the user's confidential information.
- Owner maintain the data integrity over the cloud.
- Apply data mining techniques on available datasets that improves the overall health of the growing population.
- The Proposed System assist clinicians at the point of care, it can also help in various organizations who needs to transfer secret data.
- Reducing communication overhead.
- Preserving privacy of patient's data.

## VI.CONCLUSION

Hyperledger composer is the open development tool set and framework that allow us to develop a blockchain application and integrate with the existing business system easier. By the way in our application enabled clinic records benefit individual by enabling interoperability if
clinical details a patient characteristic between clinics or hospitals and allowing identification of each patients who need to follow up for specific conditions and improves coordination care.

## REFERENCES

1] Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework. @2018 IEEE

2] Hyperledger's Fabric Composer: Simplifying Business Networks on Blokchain. Oct 2018. [online] Available: https://medium.com/@RichardCuica/hyperledgers-fabric-composersimplifying-business-networks-on-blockchain-94313b979671.

3] Hyperledger Fabric Blockchain: Chaincode Performance Analysis. Luca Foschini, Andrea Gavagna, Giuseppe Martuscelli, Rebecca Montanari Dipartimento di Informatica – Scienza e Ingegneria, University of Bologna,

Viale Risorgimento 2, 40136 Bologna, Italy {luca.foschini, giuseppe.martuscelli, rebecca.montanari}@unibo.it, andrea.gavagna@studio.unibo.

[4] M Dakshayini, Balaji Prabhu B V, "An Effective Big-Data and Blockchain [BD-BC] based decision support model for Sustainable Agriculture system", published as chapter 8 in Springer Sustainable Cognitive Computing, EAI/Springer Innovations in Communication book Series,
pp 77-86, https://doi.org/10.1007/978-3-030-19562-5_8

4] Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric. ©2018 IEEE

5] "Hyperledger Fabric," 2018. [Online]. Available:https://www.hyperledger.org/projects/fabric