iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35725

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Transfer of Secret Data using Re-encryption Technique with Hyperledger Fabric based on Blockchain Technology

Bhagyashri H. Adhau[1], Prof. Seema B. Rathod[2]
[1, 2]*Computer science and engineering Department,Sipna college of Engineering*

Abstract: ***The Personal health record system (PHR system) which stores health-records patient's information. PHR system allows the one Hospital to manage and share his/her data with selected other individuals. The originality or tamper resistance feature is crucial for PHR system because it contains sensitive information about patients. Blockchain technology with the personal blockchain becomes a potential, great solution due to its immutability properties. Unfortunately. This work aims to propose a blockchain-based PHR model. The proposed model is built using the Hyper-ledger Fabric concept to support a tamper resistance feature. Re-encryption and other cryptographic techniques Such as Advanced Encryption Standard and Hashing algorithms are employed to preserve privacy. The proposed model include flexible access control, security concerns, auditability. A detailed security analysis of our model shows that the it is provably secure for Security and privacy preserving.***
Keywords: Hyper-ledger Fabric, Personal blockchain, re-encryption

I. INTRODUCTION

A blockchain is a distributed ledger or database system for recording history of transactions on a shared data, 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). Firstly Popularized for crypto-currencies such as Bitcoin, it is public blockchain which publicly shared all data with the all users in the network. 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.

As bitcoin is a public blockchain there is a problem when some of the nodes or user want to shared data secretly and the data must be between that respected users only. 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. The participants that are allowed to share the data or information between them only, in Hyperledger Fabric are called peers (and typically there are only a few of them) and the data is seen and access between sender and receiver only no other than them can see the data or communication between them. This setting makes it easier to control the transaction, and is typically faster than public blockchains that are used in most crypto-currencies.

II. LITERATURE REVIEW

1) SOLIDUS. Solidus is a system for confidential transactions on public blockchains, aiming to hide not only the details of the different transactions but also the participants in those transactions. Designed for banking environments, it uses publicly-verifiable Oblivious-RAM (which combines ZKPs with Oblivious-RAM) to hide the identities of the individual bank customers. Similar to other ZKP-based solutions, Solidus is designed for settings where each transaction depends only on secrets of one participant (i.e., one of the banks).

2) 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.

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

4) Sandro Amofa et.al [2] have presented the Blockchain supported approach for managing the access to ehealth data protecting the privacy. This paper also presents the information about how the medical data is shared between health organizations using access policies defined by the patients. In order to protect health data, solution proposed involves the use of two types of chains: a private one, which keeps real ID of the patient's information, and a public one, which stores information about patients' health data with a temporary ID.

5) 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.

6) Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher[6] it is proposed a blockchain-based healthcare system that integrates the patients, medical sensors, doctors and hospitals. The data are stored outside blockchain to enhance the performance, whereas the blockchain is used to store only part of data or a pointer to it.

III.PROPOSED SYSTEM

A. Re-encryption Technique

The re-encryption scheme is a symmetric cryptosystem that enables its users to share their decryption capabilities with others. The Data that is identified by doctor that it is sensitive suppose contact number etc. that is encrypted and that encrypted data is re-encrypted again. Advanced Encryption Standard (AES) Symmetric block cipher is use for this cryptography and one key is shared as it is easy and possible to decrypt two times with one key.

1) Advanced Encryption Standard: Advanced Encryption Standard Symmetric key block cipher which uses same key for encryption and decryption. It takes fixed size of block size as a input = 128 bit =16 bytes =4 words as a plaintext

2) AES Algorithm

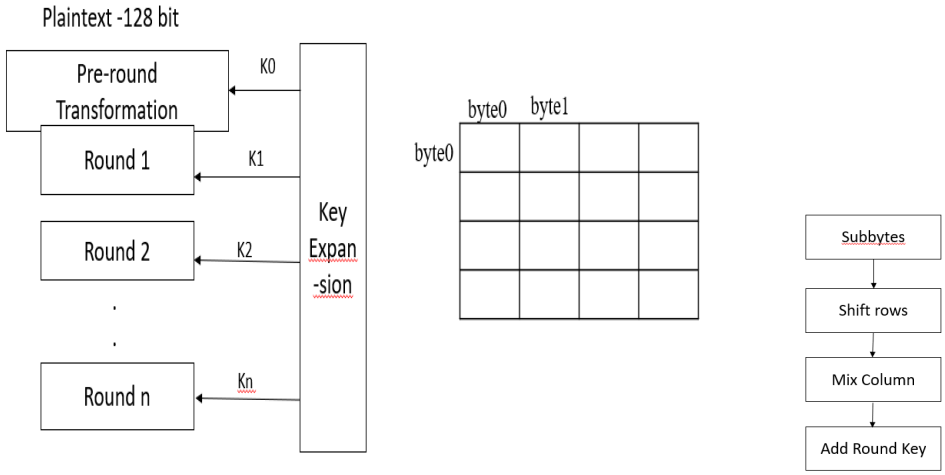


Figure 1: Re-encryption by AES Algorithm

B. Hyperledger Fabric

Hyperledger fabric is framework provide by IBM blockchain developers which with the help of docker Desktop run the Hyperledger request of push and pull to create a network. After network is created it cleans the network by passing the command through docker and networks gets cleans. After that load the client address Then can add a node and in that register hospitals.

1) In fisrt step generate Clinical Document architecture CDA: After generating it gets stored in the D drive of the user machine and with the fabric framework using create file containing meta data about the information which is to be shared.

2) In The Second Step, Upload That Cda On The Server And Then It Is Ready To Send: Data must be shared securely for that the hash code is use by the private blockchain that is hyperledger fabric in our project when we upload the file hash code is generated if file is securely transfer then Hash code is received as it is. And if it is not received securely then hash code is get altered and receiver immediately get notified that data is get altered.

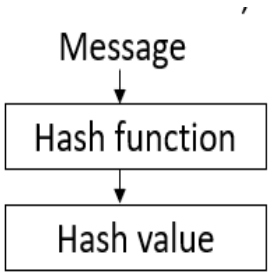
C. Hashing Function

1) Secure Hash Algorithm: Secure hash Algorithm SHA 256 Also called as compression function It Convert input into another Compressed value. Execute same file as many as times we get the sesame result but any single digit change gets a complete change in hash value.

Use checksumSHA256; function for Generating hash code of the information.

a) Deterministic how many times any time output gets same.
b) Collision resistance.

Quick computation if the computation is fast then the system works more efficiently.



Take any size of input and you will get a fix size of hash value. Which is unique for every Message.

Figure 2: Hashing algorithm.

2) Flowchart

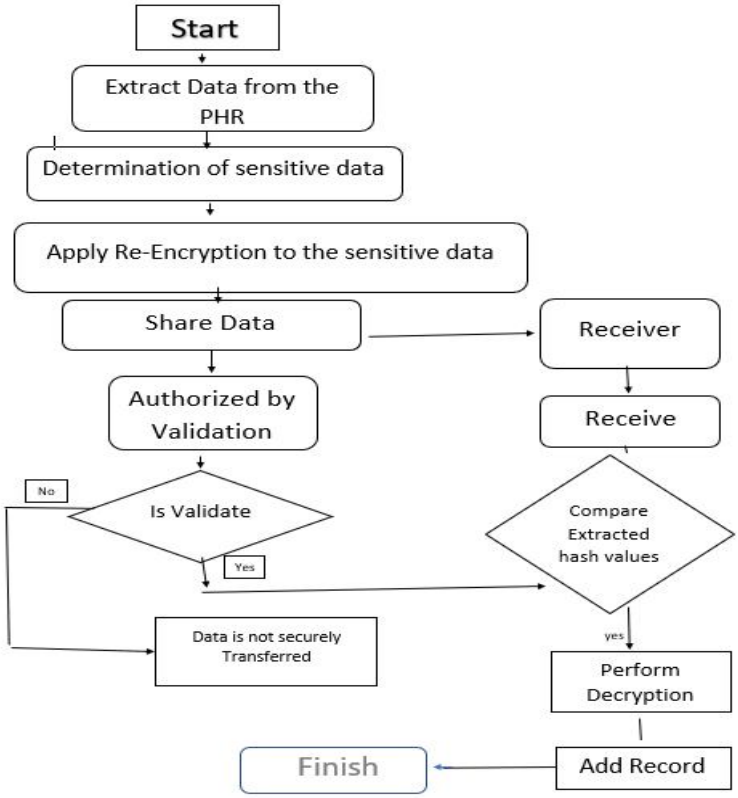
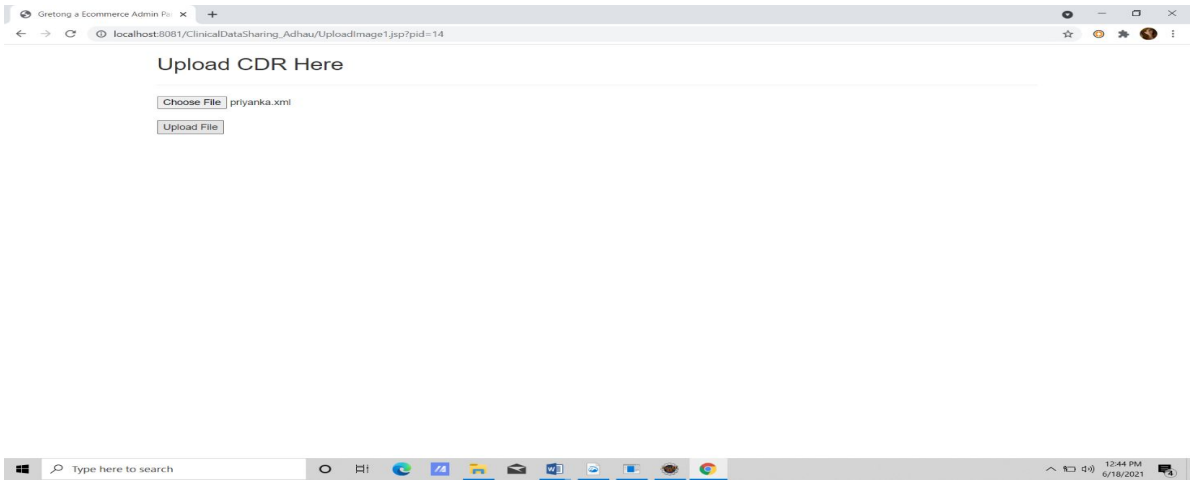


Figure 3: Block Diagram of proposed system

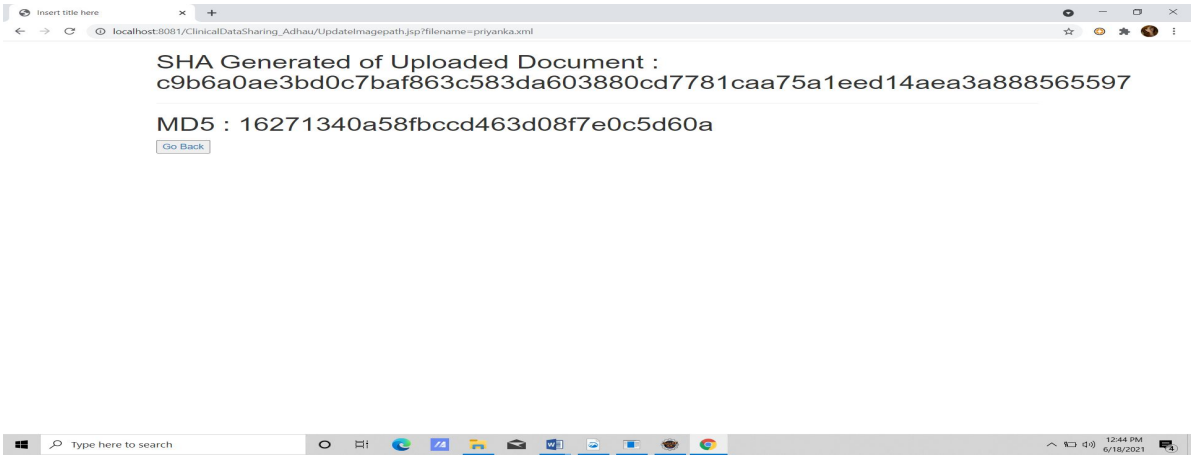
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

IV. RESULT AND ANALYSIS

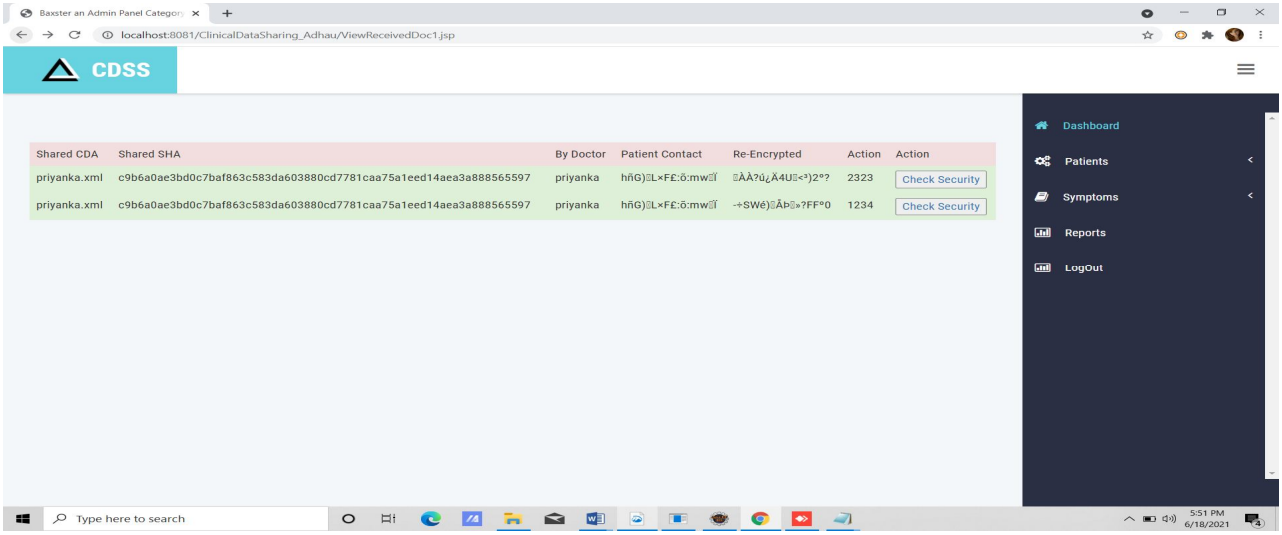
A. *After Uploading CDA*



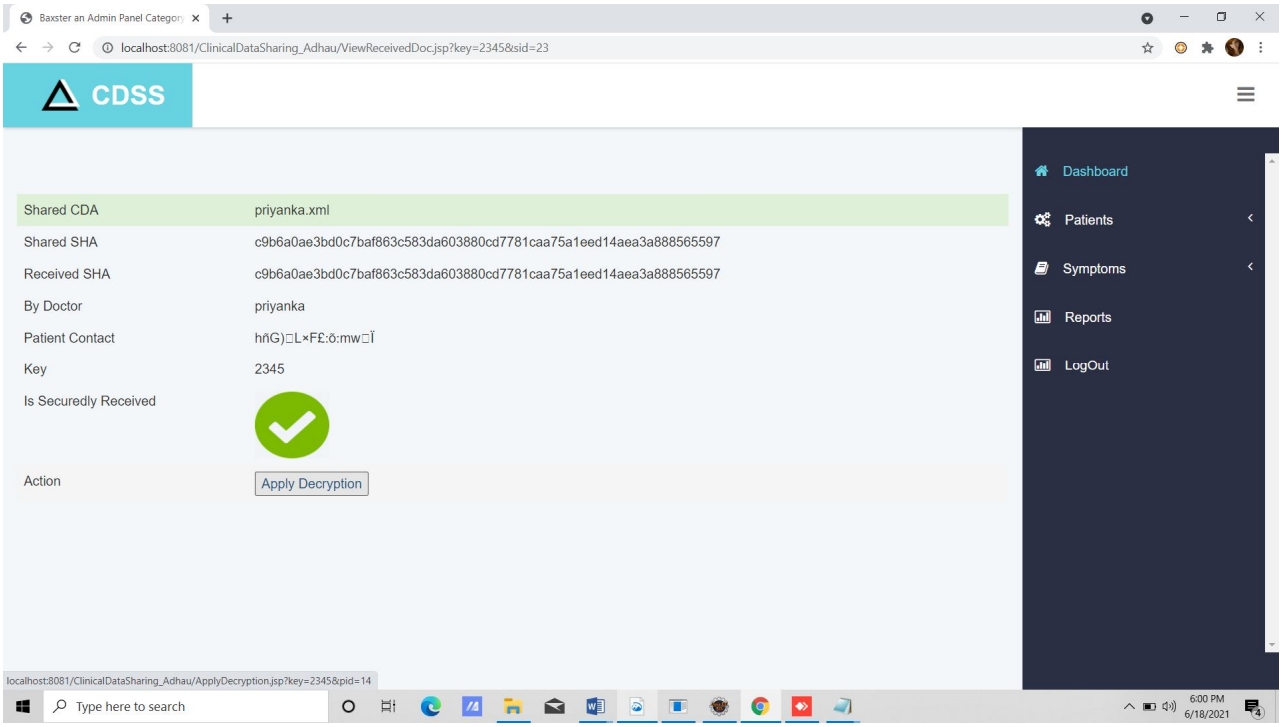
B. *The Hash Code And MD5 Code is Generated of Uploaded Document*

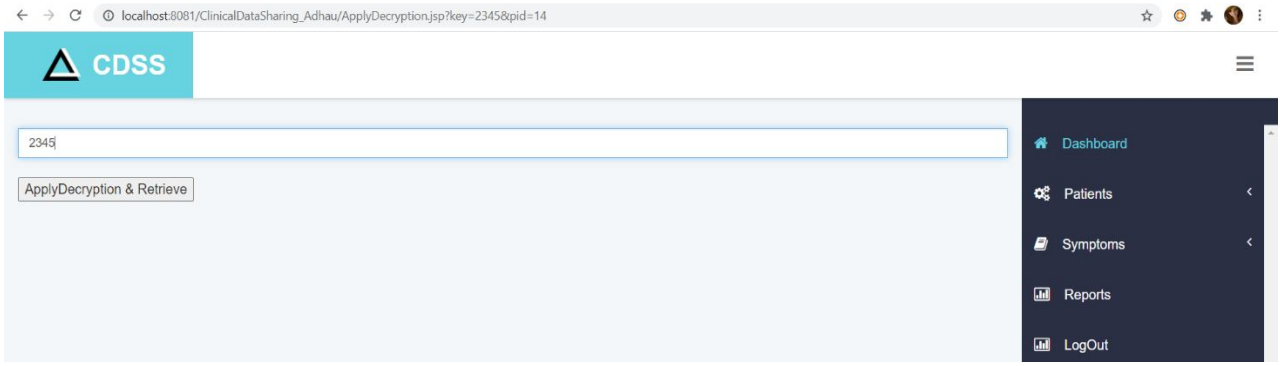


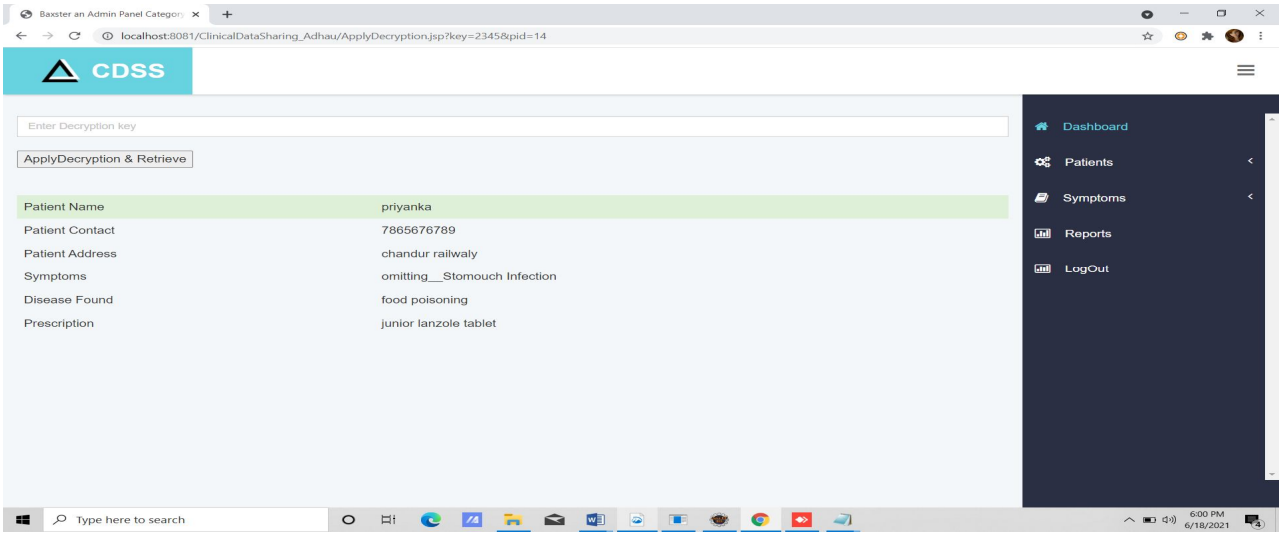
C. *After Receiving At The Receiver End He Can Check Security If Data Is Transfer Securely Or Not*



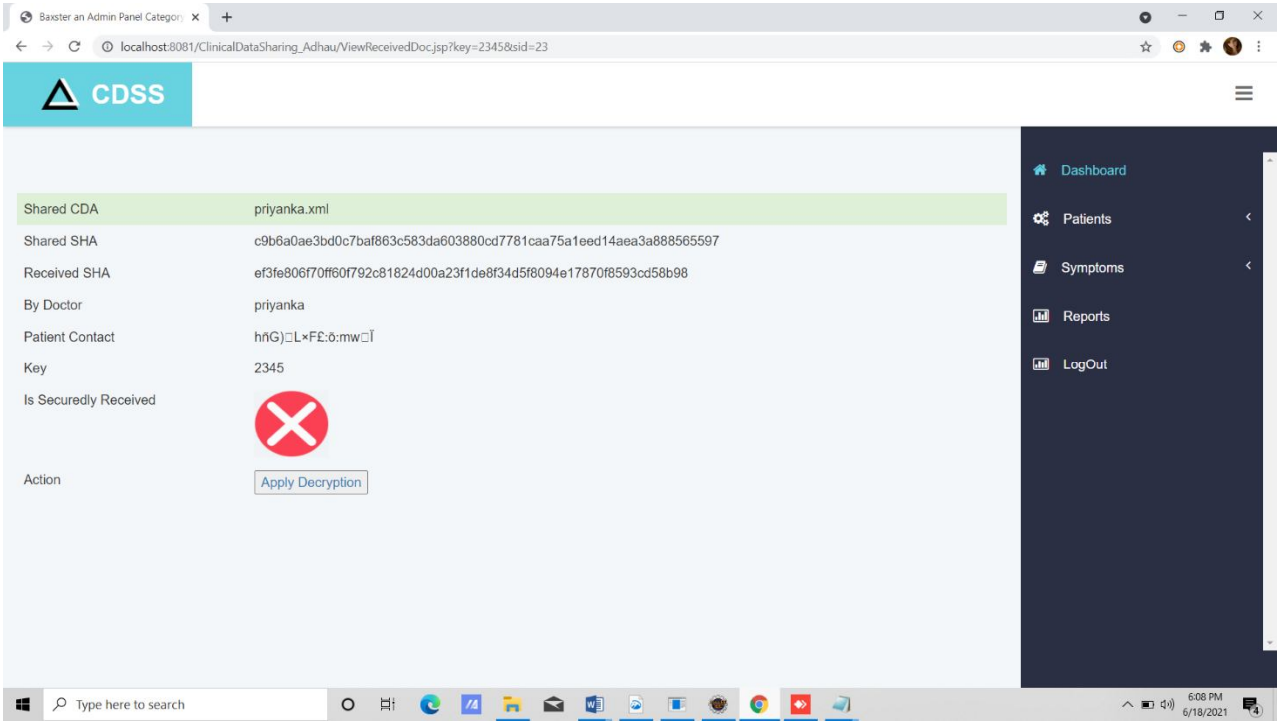
D. If Data Is Received Securely Then Output Is As Shown In Below Sreenshot







Apply decryption and get original data securely.
Meanwhile if data is corrupted or alterd or not received securely then theoutput is as shownin below sreenshot.



It means data is not securely received it is altered by someone and any single digit of change in the file will totally change in the hash code and receiver will recognized that data is alterd.

Performance test has been done by, introducing functions for automatically generating a large amount of data, and for measuring the execution time. Their purpose of that is to test the performance of the system and the ability to handle a large amount of data, the execution time, and the correctness of software modules implementation. In the following, tests that take into account the time needed to identify the medical data for a given patient, and the propagation time to all the blocks within the peer to peer network.
The Existing Health Record sharing model machine's operating system is Linux Ubuntu, and the technical features are i7 1,8 GHz 2 core processor and 8 GB RAM. Which is more costly,complicated and time consuming ,whereas we try to built a model on windows with a help of docker desktop to use some features of linux operating system and can be user friendly no special requirements of operting system can run on i3 processor with 4GB RAM. We added the Re-encryption cipher text to make it more secure . Figure 5 presents the results, of the test of existing method that measures the time needed to identify medical data for a given patient. Axis OY represents the time it takes to find the patient's records (in milliseconds), and the OX axis represents the number of records stored in the database.

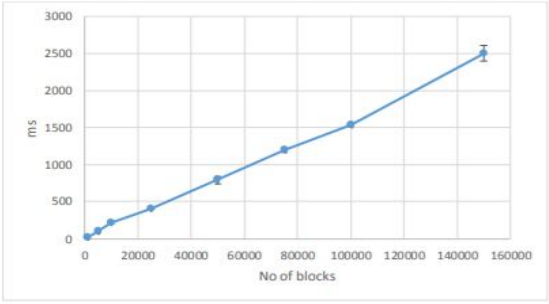


Figure 5: Time required to find the medical data of a given patient Our system takes to upload and calculating hash value of patient record 0.3 ms.

V. CONCLUSIONS

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.

PHRs play a significant role in improving patient's care and enhancing the delivery of health care services.

REFERENCES

[1] Abdelali El Bouchti, Houssine Bouayad and Youness Tribis "A Systematic Mapping Study on Supply Chain Management based on Blockchain" International workshop

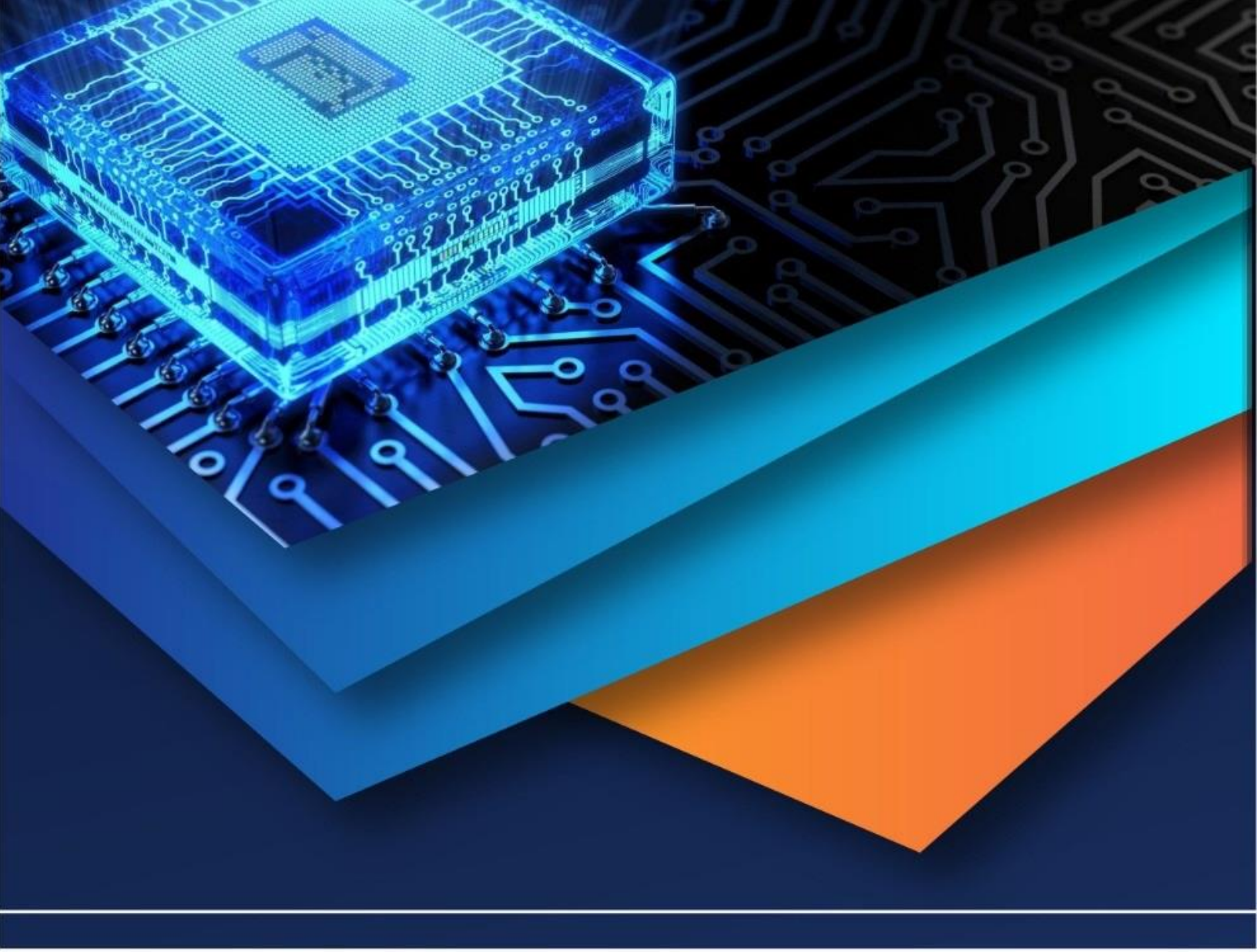
[2] Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework. @2018 IEEE.

[3] M Dakshayini, Balaji Prabhu B V, "An Effective Big- Data and Blockchain [BD-BC] based decision support model for Sustainable Agriculture system", published as Chapter8 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] A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data: Sandro Amofa, Emmanuel Boateng Sifah, Kwame O.-B Obour Agyekum, Smahi Abla,.

[5] 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

[6] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher: "Towards Using Blockchain Technology for eHealth Data Access Management". Fourth International Conference on Advances in Biomedical Engineering (ICABME), 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY