International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228416

Advanced Unified Encrypting Methodology to Enhance The Security of Health Information in Cloud Storage Employing Blockchain

Thasni K N[1], Biju Abraham Narayamparambil[2]
Computer Science and Engineering, Rajagiri School of Engineering and Technology, Kakkanad,_Kochi, Kerala, India

Article Info
Publication Issue :
Volume 8, Issue 4
July-August-2022

Page Number : 122-128

Article History
Accepted: 10 July 2022
Published: 22 July 2022

ABSTRACT

Security of health information has been a major issue in the health care industry. Health information exchange have been help doctors, patients, and other healthcare providers to securely access and share the medical information. Cloud computing led to easier and safer access and sharing of medical records. To provide additional security to cloud computing employ encryption techniques and blockchain. In this method develop the mobile application to enhance the security of health information in cloud storage using various encryption techniques and blockchain.Base64 encoding and AES algorithm are used for providing more security to the medical records. Blockchain transactions occur within a peer-to-peer network of patient records. SHA-256 algorithm is used for implementing the blockchain. This system protects the confidentiality of health data stored on cloud storage.

Keywords : Security, Encryption, Blockchain

I. INTRODUCTION

Cloud computing has become an essential part of I.T industry in the last few years. More and more organizations especially the healthcare industry adopt this cloud technology because of the large volume of data processed in the healthcare industry. cloud is economically feasible. Cloud computing facilitates and secures medical record exchange. Cloud computing enables easier and safer access and sharing of medical records. Better anywhere, anytime access to the cloud will also enable the effective use of healthcare resources and effective exchange of information. But still, no privacy and protection laws are created for cloud computing. So There is a need to secure health information locally and globally. To make cloud computing more secure employ various encryption techniques and blockchain technology.

The blockchain contains a list of records called blocks linked together by hashing mechanism. The blockchain facilitates information exchange and coordination among healthcare entities and helps patients become independent in sharing their medical records with their providers. Blockchain is a trustful distributed ledger to collect, store, analyze, and validate medical records.

The purpose of the work is to aid the healthcare industry. The advantages and disadvantages of the

different models are studied and came up with a model that effectively and securely exchanges health information. For encrypting the information use hybrid of Base64encoding and AES algorithm. Blockchain transactions of medical data are employed using SHA-256. This system helps to secure the exchange and access of health information.

The organization of this document is as follows. In Section 2 (Related Works), That will give detail study of different methods of encryption and blockchain. In Section 3 (Methods and Material), present modules in the proposed system. In Section 4(Results and Discussion) present the screenshots of the application. In section(Conclusion)a conclusion is the last part that discuss about the future scope of the proposed method.

II. RELATED WORK

In this section, the existing research work in the field of cloud technology, encryption, and blockchain is done. A detailed survey is done in different methods of blockchain and encryption techniques.

The system uses RSA for encryption. When the patient goes to the hospital the information is collected and stored in the cloud by the healthcare providers or by the doctors. Before storing into the cloud information is encrypted. The patient gets the secret key. On the doctor, side patient shares the secret key with the doctor. Using the secret key doctor can access the health information. But in this existing system, only the text information is encrypted and uses the RSA algorithm for encrypting the message. No blockchain is employed. The proposed system uses an AES encryption algorithm and base64 encoding. In the proposed system text and image data are encrypted and integrated into the blockchain. to provide more security. AES Algorithm is faster than RSA. RSA and AES are two types RSA is asymmetric and AES is symmetric. AES poses more computing power than RSA when sharing the secret key. AES requires less time for calculation with large numbers.

The system presents a symmetric key-based scheme for the mixing of networks. And also employ blockchain for achieving data integrity. There is restricted access to future health data that can be achieved by forward secrecy in the blockchain. This system achieves user unlinkability property using the presence of Mixnode. In this system for health, the record upload section uses blockchain technology to store the record in blocks. Each block has the data hash and previous hash. The Hash of the new block is computed using the hash of the data and the previous hash. This is used to maintain the integrity of the PHR document and lab report of the patient. In this system, multiple Patient records are stored in a single block thereby reducing the size of the blockchain. This system employs the mixnode technique along with the blockchain. A network that consists of set nodes called mixnode. Before sending the message the sender shuffles the message. This results in harder to trace the message between sender and receiver. When a wants to send a message sender appends a random number r0 with the message and encrypts it using the receiver's public key. The encrypted message is appended with the random number r1 once again before being encrypted with the Mixnode's public key.

On the receiving side, they decrypt the message using Mixnode's private key, discard the random number r1, and deliver the message to the receiver. The attacker cannot observe the message since the message looks different on both the sender and receiver sides. This system provides confidentiality, data integrity, user unlinkability, and efficient access to patient records.

The system, using a distributed ledger technology that is considered "unhackable."And created a blockchain model to preserve data security and patients' privacy, assure data provenance, and give patients complete

control over their health records through utilizing the smart contract technology, which is a programmable self-executing protocol executing on a blockchain. This concept delivers patient-centric HIE by customizing data segmentation and an "authorized list" for doctors to access their data. Then ran a large-scale simulation of this patient-centric HIE process and quantified its feasibility, stability, security, and robustness.The blockcain technology maintains all log files, allowing patients to always see who has accessed their data. All doctors may validate the source of EHR data, ensuring data integrity. Clinicians can only check the information entered by trusted healthcare institutions. System administrators may view the number of clinicians who have requested data from their healthcare institutions. In addition, storing log files in smart contracts can help with health data administration. The benefit of this strategy is that it reduces the risk of data breaches and ensures data consistency. The disadvantage of this strategy is that it requires at least one node to connect to the blockchain Scalability restrictions from the blockchain.

The system presents a cryptographic blockchain technique based on the md5 hash algorithm. The method makes it difficult to change data without The strategy makes it impossible to modify data without being detected and employs a distributed approach combined with blockchain. In this system, the MD5 algorithm was utilized to validate and authenticate the medical data that was recorded for analysis. It is the most widely used Hash security algorithm in message confirmation, reputation finding, and so on. The message is divided into 512 piece input squares by the algorithm. Each square is subjected to a movement of abilities in order to create an unusual 128-piece message that separates the message into 512-piece input squares. Each square is subjected to a movement of abilities in order to create an unusual 128-piece statement. The method requires a message length of 8 bits. This system require more time for validation.

The system proposes Blockchain Technology as the greatest approach to handle all problems and meet all demands. Blockchain, as a decentralized and distributed ledger, has the potential to affect billing, record sharing, medical research, identity theft, and financial data crimes in the future. The use of smart contracts in health care can further simplify matters. On Blockchain, invocation, record generation, and validation will take place. This system focuses on the patient-driven model of record maintenance utilizing Blockchain technology, where smart contracts can be added in the future to increase data interchange potential. Blockchain Innovation A blockchain is a distributed, immutable, shareable, and tamperproof data structure that stores a constantly expanding list of transactions. Each block has its own identification, which is known as a cryptographic hash. The hash value of the block that came before it is sent to each block. As a result, a connection is formed between the blocks, resulting in the formation of a chain of blocks. This transaction is published to the Blockchain network and validated by miners. Miners are Blockchain nodes with high processing power. Miners use a consensus mechanism known as Proof of work to ensure that the transaction is unmodified and irreversible. There is a race among miners to create a legitimate block, and the person who does so is rewarded.

III. METHODS AND MATERIAL

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. System Architecture

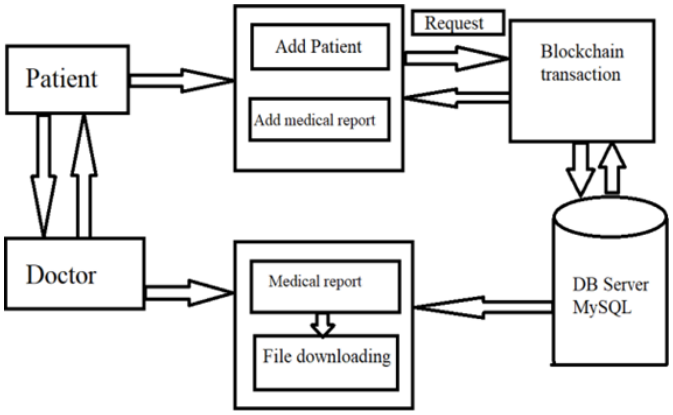


Figure 1 : Architecture

When the patient goes to the hospital for treatment the details of the patient are collected by the healthcare providers or by the doctors. And the information is encrypted and stored in the cloud. After adding the health information get the encryption key. For encryption use the techniques, base64encoding and AES encryption algorithm and also employ the blockchain transaction for medical data. When the patient goes to the doctor's room patient has to share the secretkey with the doctor. The doctor can access the medical information by using the secret key and provide the treatment.

B. Module Overview

The proposed architecture is divided into two modules:

- Patient
- Doctor

Level 0 :

Figure 2 : Level 0

Level 0 shows 2 modules in this system patient and doctor. Patients exchange health information with the doctor. Doctors access health information.

Level 1-Patient:

The level 1 patient as in figure, patient login into the application using an email id as the username and password given during the registration process. After entering into the application patient have the following options.

- To add patient records
- To add medical records
- To upload image and file
- To view the patient list
- To view the medical records in encrypted form
- To view the medical records in original form
- To view the transaction of medical report

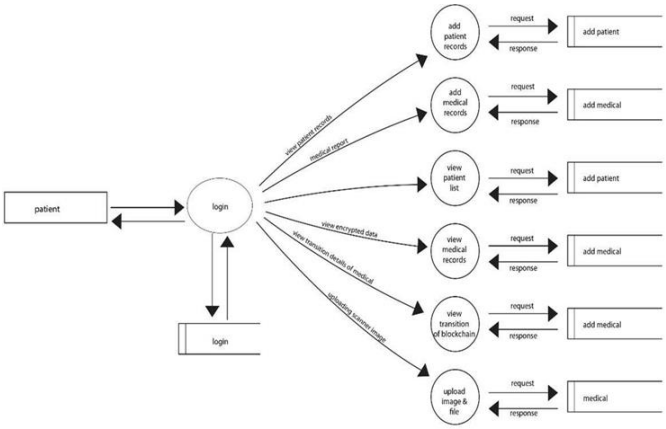


Figure 3 : Level 1-Patient

Level 1-Doctor:

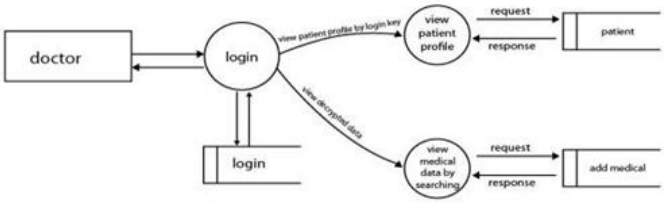


Figure 4: Level 1-Doctor

The level 1-doctor, the doctor login into the application using the patient id as the username and an encryption key gets from the patient as the password. After entering into the application doctor has the option to view the patient profile and to view

the medical information by searching the encryption key.

ER-Diagram:

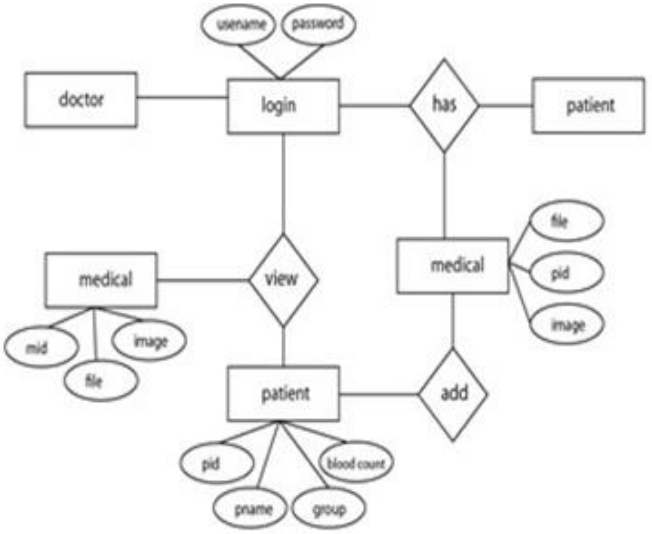


Figure 5 : Entity Relationship Diagram

Entities are things or concepts that represent vital information. Nouns such as product, client, location, or promotion are examples of entities.Entities in entity connection diagrams are classified into three categories. In our system, the Patient and Doctor are viewed as separate entities, each with their own login credentials. The medical report isalso regarded as an entity.

Relationships are used in entity-relationship diagrams to document the interaction of two entities. Relationships are generally verbs like assign, associate, or track and give important information that entity types alone cannot supply. In the suggested scheme, Relationships involving patients and medical reports. Assign medical reports to each patient individually. This grants the patient authorization to upload and read medical reports Also, build contact with the doctor and obtain medical records. This gives the doctor permission to read the medical reports.

Entity Relationship Diagram attributes are entity properties that assist users in better comprehending the database. Attributes are used to incorporate information about the different entities indicated in a conceptual ER diagram. The login entity has the prop- erties username and password. Medical reports contain the patient id, picture data, file, and patient entity, which includes the patient id, patient name, blood group, and blood count, among other things.

usecase diagram:

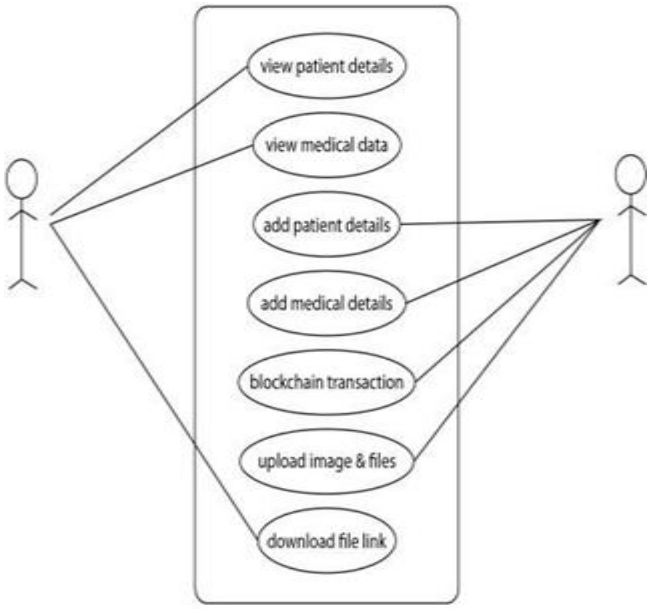


Figure 6: Usecase Diagram

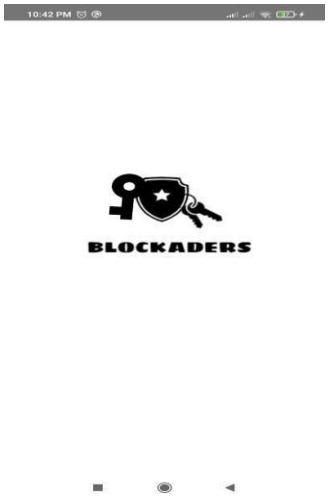
As seen in the DFD of level 1-patient and level 1-doctor usecase diagram shows the granted options for both the patient and doctor. In figure 3, the first user is the doctor and the second is the patient. On the doctor's side who has permission to view the medical records. Medical reports contain three types of data that contain text, image, and file links. The doctor has permission to download the file using that link.

Dataset:

Dataset include the text data of the patient,image data of the patient and the file.

- Text data has two part
- Basic data - patient name, age, address, email, contact number, etc.

- Medical data –Blood group, cholesterol level, HB count, etc.
- Image data -patient photos or medical images.
- File -CT report or MRI report, etc.



Hardware Requirements :

- Android version 8 or above :
- Processor:1.2 GHz or faster
- Storage:32 GB
- RAM:2 GB
- Main Processor: Intel core i3 or above
- RAM: 8 GB or Above
- Hard disk: 10 GB of available disk space minimum or above

Software Requirements:

- Operating System : 64-bit Microsoft Windows 10/11
- Programming Language: Java, Android
- RDBMS: MYSQL
- Web Server: Apache Tomcat & Glassfish Server
- Scripting language: JSP

This method requires encryption and blockchain technique. It is implemented in windows and android mobile. Collect the details of the patient both the basic and medical data. Basic information about the patient is encoded and medical information is encoded and encrypted. For encoding use base64 encoding and AES encryption for the encryp- tion process. Also requires SHA-256 for implementing blockchain technology.

IV. RESULTS AND DISCUSSION

The system is implemented and is able to secure the health information stored on the cloud. The health information may be text data, image data, and files. There are two modules namely doctor and patient and treated as different entities. Patients and doctors have different logins.

Figure 7 is our application. Then goes to the login page. where both the patient and doctors can login into the application using different login.

Figure 7 : Main Activity

Cloud Storage Employing Blockchain login into the application register the details of patients and doctors. where we can add name, email, phone, address, and password. After the registration sign into the application.

The registration page for the patient and doctors are shown in figures 8 and 9 respectively.

Figure 8: Patient Registration

Figure 9 : Doctor Registration

On the patient login page as shown in figure 10 where we can login into the application by using email id as the username and the password that is given during the registration page. Then we enter into the application and there have an option to add the patient records and medical records as shown in figure 11.

Figure 10 : Patient Login

There are 4 bottom navigation options in the patient module as seen in figure 11. The first one is for adding the details of new patient basic data as well as medical data. The second option is for viewing the patient's name. On clicking the name of the patient view the medical data in an encrypted format. The third one is for blockchain transac- tions of medical records. The last option is for viewing the medical data in the original form.

Figure 11 : Patient Data Upload

In The first option as seen in figure 11, there are two options one for adding patient basic data and the other for adding medical data. On clicking the patient button where we can add basic details patient as seen in the figure 12. After adding the basic details get the encryption key that is seen in the figure 13.

Figure 12: Patient Basic Data Upload

Figure 13: Encryption Key

After getting the encryption key to add the medical data as in figure 14. On this page add the text medical data such as blood group, cholesterol level, HB count, etc. There have an option to capture the image of the patient and also an option to upload the med- ical images such as CT scan images or MRI scan images etc and to upload the link of medical files such as CT scan reports or MRI scan reports etc.For adding patient medical data select the patient name.

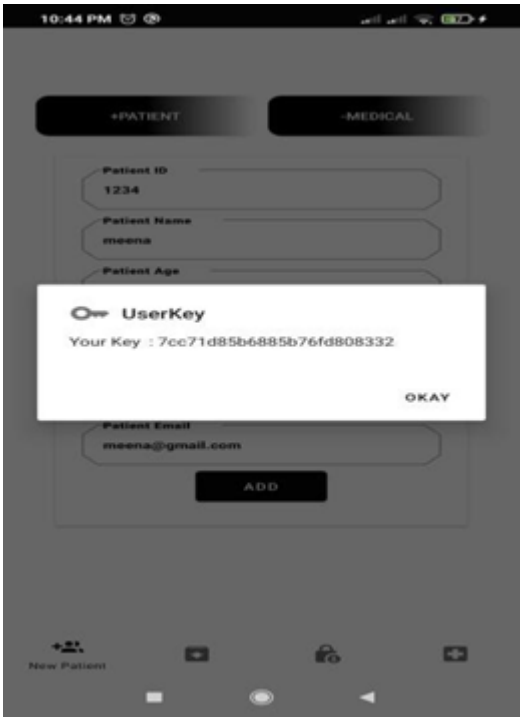


Figure 14 : Patient Medical Data Upload

After adding the medical data of the patient we can see medical data in an encrypted as well as in the original format as shown in the figure. For viewing the medical data in an encrypted format first select the name of the patient as shown in figure 15. In the figure 16 of encrypted data first, part is encrypted text for medical images second part is the encrypted form of text medical data. The last part is the encrypted text for the link of the file.

Figure 16 : Patient Encrypted Data

The option for viewing the blockchain transaction of medical data is shown in the figure where we add the encryption key get after adding the basic details of specific patients. After adding the encryption key click on the request button. when the patient id is valid the block will display. That is shown in figure 17.

Figure 17 : Blockchain Valid True

In figure 17 there is a viewmore button. when pressing the view more button we can view hash values of the data, previous hash, timestamp, and nonce as seen in the figure 18.

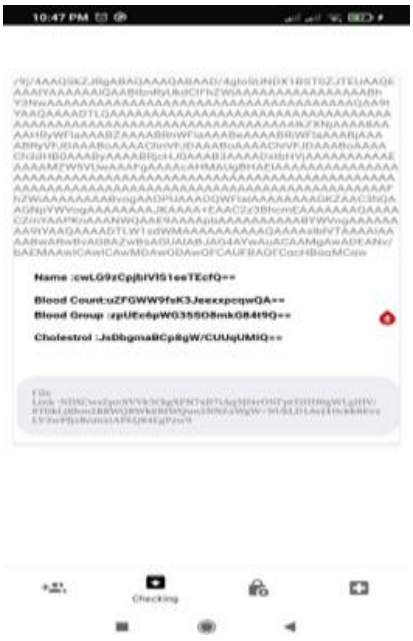


Figure 18 : Hash Computation

In that, there is an option to hide the hash values.
For hiding the information press the hide button.
If the blockchain is not show the message blockchain false and transaction failed as shown in the figure.The logout option is also in the page of blockchain,lock image as seen in figure 19.

Figure 19 : Blockchain valid False

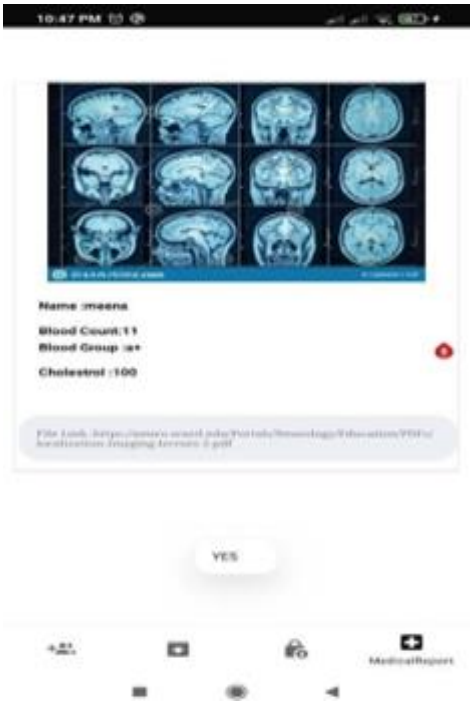


Figure 20: Patient Medical View

DOCTOR MODULE:
The doctor login into the application by email as the username and the password thenenters the application as shown in figure 21.

Figure 21 : Doctor Login

After entering into the application doctor can view the list of patients that shown in figure 22.

The last option in the bottom navigation include the patient medical information as seen in figure 20.

Figure 22 : Patient List

When clicking on the patient name goes to the next page as in figure 23.

Figure 23 : View Options

The above page contains two options one for viewing the patient profile and the other for viewing the medical records by searching by the encryption key as shown in figures 24 and 25.

Figure 24 : Patient Profile View

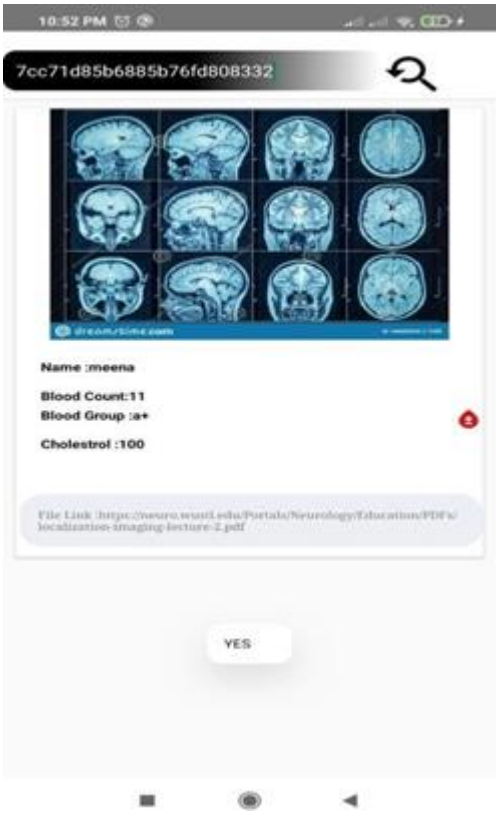


Figure 25: Doctor Medical View

From the link given on the medical information page. Can download the files. That is shown in figure 26.

Figure 26: File Download

If the encryption key is not valid. Then display the message no medical data found that is shown in figure 27.

Figure 27: No Medical Data

permission in android is solved with an easy permission class. In future work, planning to overcome these challenges. This approach is intended for the enciphering and deciphering of textual data and the image-oriented data-set of the healthcare industry. Ensure patient privacy using the blockchain security model. In future work integration of quantum computing would be considered. Quantum computing is an emerging technology of computing that works on the principle of quantum mechanics, which solve too complex problems. Quantum computers are not capable to break the encryption keys. To break the security quantum computers require 1000 times the computing elements. So the integration of quantum computing would increase the efficiency of the system.

Discussion

The patient, the module adds the details of the patient both basic and medical data. After adding the basic details of the patient generate the encryption key.

The basic information of the patient is encoded using the Base64 encoding scheme. The medical information of the patient is encrypted using Base64 encoding and AES encryption algorithm. For employing blockchain transactions for medical information use the SHA-256 Encryption algorithm.

V. CONCLUSION

In recent years, the use of blockchain techniques for the secure transactions has come up with great interest. In this paper, developed a mobile application for uploading the health information of the patient and securing the health information stored in the cloud by Base64 encoding and AES encryption Algorithm, and employ blockchain for medical data transaction. In this method doctors can access the health information without any corruption in the uploaded data. This system protects health information from unauthorized users and also provides the confidentiality of data in the cloud. So this method can be made applicable to real-world hospital systems to make them more secure. The main limitations of this proposed method is that server remains live at all time and storage.

VI. REFERENCES

[1]. M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[2]. Rituraj and N. Kumar, "Cloud-based Secure Personal Health Record Management System using Mixnode and Blockchain," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4),2020,pp.7075,doi:10.1109/WorldS450073.2020. 9210317.

[3]. Y. Zhuang, L. R. Sheets, Y. -W. Chen, Z. -Y. Shae, J. J.

[4]. P. Tsai and C. -R. Shyu, "A Patient-Centric Health Information Exchange Framework Using Blockchain Technology," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169-2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.

[5]. R. N. A. Sosu, K. Quist-Aphetsi and L. Nana, "A Decentralized Cryptographic Blockchain Approach for Health Information System," 2019 International Conference on Computing, Computational Modelling and Applications (ICCMA), 2019, pp. 120-1204, doi: 10.1109/ICCMA.2019.00027.

[6]. V. B, S. N. Dass, S. R and R. Chinnaiyan, "A Blockchain based Electronic Medical Health Records Framework using Smart Contracts," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4, doi: 10.1109/ICCCI50826.2021.9402689.

[7]. Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte School of Electronics and Communication Engineering REVA University, Bangalore, India "Health Record Management through Blockchain Technology " Proceedings of the Third International Conference on

[8]. Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386- 9439-8

[9]. Q. Huang, W. Yue, Y. He, and Y. Yang, “Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing,” IEEE Access, vol. 6, pp. 36584–36594, 2018. Project Report Advanced Unified Encrypting Methodology To Enhance The Security Of Health Information In Cloud Storage Employing Blockchain

[10]. R.Swathi, T.Subha “enhancing data storage security in cloud using certificateless public auditing” 2017 IEEE

[11]. R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, “Flexible and efficient

blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system," IEEE Access, vol. 7, pp. 88012– 88025, 2019.

[12]. R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy ensured Ehealthcare for fog-enhanced IoT based applications," IEEE Access, vol. 7, pp. 44536–44543, 2019.

[13]. B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5 th International Conference on Advanced Computing Communication Systems (ICACCS), 2019, pp. 699-703, doi: 10.1109/ICACCS.2019.8728483.

[14]. D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," in IEEE Access, vol. 9, pp. 158122-158139, 2021, doi: 10.1109/ACCESS.2021.3130552.

[15]. N. Kumar S. and M. Dakshayini, "Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI),2020,pp.15,doi:10.23919/ICOMBI48604.2020.9 203442.

[16]. M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem, "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257720.

[17]. V. Mahore, P. Aggarwal, N. Andola, Raghav and S. Venkatesan, "Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain," 2019 IEEE Conference on Information and Communication Technology, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.

Cite this article as :

Thasni K N, Biju Abraham Narayamparambil, "Advanced Unified Encrypting Methodology to Enhance The Security of Health Information in Cloud Storage Employing Blockchain ", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 4, pp. 129-141, July-August 2022. Available at doi : https://doi.org/10.32628/CSEIT228416

Journal URL : https://ijsrcseit.com/CSEIT228416