International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure blockchain assisted of Medical Things using Identity based Encryption Scheme for High Data Security

[1]D. Baby Sathiya, [2]Dr. L. Nalini Joseph

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Through the use of wireless networks, the Internet of Medical Things (IoMT) facilitates communication between patients and healthcare professionals. Consequently, similar to many other Internet of Things (IoT) devices, IoMT devices do not have adequate security protections. Every time a doctor and patient conduct business, our technology utilises a blockchain to encrypt their sensitive medical information. Additionally, the doctor is able to submit the therapy to the blockchain with the assistance of this method. Every time a doctor and patient conduct business, our technology utilises a blockchain to encrypt their sensitive medical information. Additionally, the doctor is able to submit the therapy to the blockchain with the assistance of this method. The study uses the idea of Identity Based Encryption management with blockchain technology. Users protect themselves from fraud and identity theft with the help of the Identity based Management system's encryption features. By integrating these technologies, the data storage process can be made more secure and safeguard the privacy of the IoMT. This approach is simply modified to enable search capabilities. Lastly, the efficiency and effectiveness of the proposed schemes is verified by comprehensive performance assessments and security studies.

Keywords: *Internet of medical things, Blockchain, Security,*

I. Introduction

Patients benefit greatly from access to accurate medical records. New medical treatment for each patient is necessary to document their medical history since, in the present medical systems of different institutions, much of this information cannot be used interchangeably. Sometimes, the only way to get data is to rely on generalised memories. Paper medical records are still used by the majority of hospitals; however, they are prone to damage and loss, making them an inaccurate way of documenting medical information. All of the system's nodes, operations, and transactions benefit from blockchain technology's distributed ledgers. Data privacy, nonrepudiation, and integrity can be achieved via electronic signature technology and identity-based encryption. Cyberspace information is more transparent, behaviour is easier to monitor, and all nodes contribute data.

We are now living in the digital age, and with the growth of IoT technologies comes a host of design considerations for organisations about privacy. Healthcare organisations have an ethical and legal dilemma when it comes to patients' medical data, which makes security a challenging subject to handle. Preliminary research indicates that blockchain technology can provide a significant solution to the data security problems affecting the Internet of Things. Therefore, when developing a blockchain strategy for healthcare applications, it is essential to guarantee data security [1].

New opportunities for remote health data analysis to achieve smart healthcare have emerged with the expansion of the Internet of Things (IoT). However, due to the sensitive nature of medical records, safeguarding patients' data privacy seems to be a

Research Scholar, Department of Computer Science,
Bharath Institute of Higher Education and Research, Chennai-73.
Professor, Department of Computer science,
Bharath Institute of Higher Education and Research, Chennai-73
Email: babysathiya10@gmail.com

tough task. Storing sensitive patient data on servers owned by other parties poses serious threats to data privacy.As long as patients' privacy and security are paramount, sharing EHRs can improve the reliability of diagnoses. One potential solution to facilitate secure and private sharing of individual health records is blockchain technology, which has many advantages, including immutability [2].

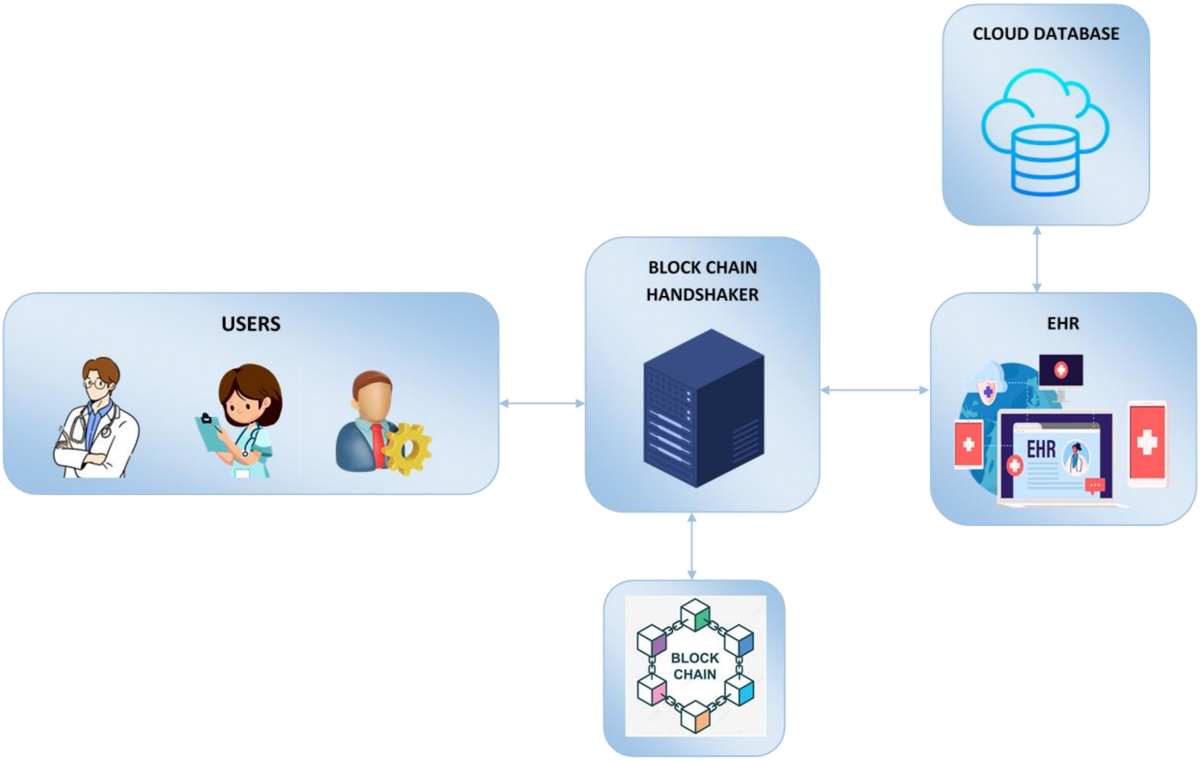


Fig.1 Block chain based Electronic Health Record Storage

By using a wide range of sensing devices and communication protocols, the Internet of Things (IoT) enables interactions between numerous entities. The Internet of Things (IoT) is an expansion of the current Internet that decreases the need for human participation in information exchange by transmitting data acquired by terminal devices over different communication protocols. In order to improve people's quality of life, the Internet of Things (IoT) is used in various smart home, smart city, and e-healthcare applications. The medical industry has recently made use of a number of new information technologies to speed up development in a number of areas related to the IoMT. In IoMT, doctors do more than just keep tabs on their patients' vitals using various data collecting tools; they also confer with them remotely, perform procedures on them from afar, and more. Better integration and sharing of medical resources between patients and clinicians is possible with the advent of the IoMT. With an emphasis on ancillary imaging and pathology diagnosis, auxiliary nursing, auxiliary follow-up, intelligent hospital administration, and auxiliary health management, Artificial Intelligence (AI) has been experimentally used in the medical and health domains. Thus, the Internet of Medical Things (IoMT) powered by artificial intelligence represents a sea change in healthcare that will undoubtedly advance medical technology [3].

A platform known as BlockRx has been successfully implemented in real-world applications. Integrating blockchain technology with Solve's robust digital ledger technologies makes the system what it is. Research and biomedical organizations' health information is included into the platform. From its first implementation to its current state, Block Rx has come a long way. [4] Blockchain is a powerful network that can enhance healthcare systems and operations by providing very efficient data and maintaining trust. The integration of many notable aspects, such as decentralized storage, accessibility, data integrity, authentication, data access flexibility, connection, and safety, enables the greater application of blockchain technology for healthcare data management. Using the principle of "smart contracts," which are universally accepted by all participants in the healthcare system, blockchain technology eliminates the need for a middleman by defining conditions and laws that are binding on all parties. It reduces unnecessary administrative costs [5].

The goal of establishing a safe system that utilizes blockchain technology and an Identity-Based Encryption (IBE) scheme for Medical Things (e.g., medical equipment, patient records, etc.) is to guarantee that all data related to healthcare is secure, private, intact, and easily accessible. Additionally, a strong system is to be built that safeguards private medical information, guarantees regulatory compliance, promotes interoperability, and builds confidence among all partners in the healthcare system. Preventing breaches, unauthorized access, or manipulation with sensitive medical data is of utmost importance. Data kept in a decentralized way is more secure and less susceptible to manipulation or unauthorized alterations when a blockchain-assisted system is put into place.

II. LITERATURE SURVEY

For the purpose of addressing the issues of blockchain-based cloud centric IoMT healthcare systems, such as high latency, high storage costs, and single point of failure, Bhaskara S et al. [6] presented a hybrid computing paradigm that incorporates a blockchain-based Distributed Data Storage System (DDSS). To enhance the security capabilities of the proposed system, a decentralized SRAC mechanism is implemented, which is based on rings that control access. Algorithms are included to authenticate devices and encrypt patient information. Through the use of Blockchain technology, the efficiency and cost-effectiveness of data sharing are accessed on the proposed system. As an added bonus, a logical system analysis is ran that proves our privacy and security methods based on architecture can handle the demands of decentralized IoMT smart healthcare systems. Experiments show that our Fortified-Chain based H-CPS offers decentralized automated access control, privacy, and security with a reaction time of milliseconds and minimal storage requirements compared to conventional centralized H-CPS.

To provide safe search and keyword-based database access, Aitizaz Ali et al. [7] suggested blockchain as a decentralized database that uses a homomorphic encryption method. In addition to revising different rules as needed, the suggested method also includes a safe way to revoke keys. This led to the development of a safe system for patients' medical records that combines blockchain technology with trust chains to address the shortcomings of existing systems for exchanging digital health records in terms of both efficiency and security. As a result, our suggested method offers cost-effectiveness, increased efficiency, and transparency. Simulations are ran using Hyperledger Fabric, a blockchain-based platform, and OrigionLab, an assessment and analysis tool. The outcomes of the proposed suggested models are ran with those of the reference models. The results of our comparison show that the healthcare system is better protected by our suggested framework, which also has a searchable mechanism.

Secure search-able blockchain, a distributed database that uses homomorphic encryption to allow users to safely access data via search, was created by Aitizaz Ali et al. [8] using deep learning. The inclusion of secure key revocation and update rules in our proposed research is becoming more important. The proposed access control mechanisms were tested and compared to benchmark models using an IoT dataset in this study. The hyperledger tool makes use of smart contracts to execute the suggested algorithms. There is a comparison to current strategies in order to assess the proposed one. Our proposed method outperforms benchmark models in terms of efficiency while simultaneously improving security, anonymity, and user behaviour monitoring for blockchain-based IoT systems.

For EMRs, Jingwei Liu et al. [9] suggested a blockchain-based inner product searchable encryption method with multi-keyword search (MK-IPSE) to provide complete privacy preservation and efficient ciphertext retrieval. In addition to enabling access policy concealing, inner product encryption (IPE) allows users to establish access rights so that only users with specified characteristics can access the target files. In addition, the suggested method integrates searchable encryption (SE) with federated blockchain (FB) to provide dependable and effective multi-keyword searching. The computation and storage performance of MKIPSE is superior than that of the current systems. Furthermore, our method can withstand IND-CKA and collusion attacks, according to the security study.

Patients, research institutions, and semi-trusted cloud servers can all benefit from the safe exchange of medical data according to a new privacy-preserving technique suggested by Haiping Huang et al. [10]. Additionally, it ensures that both patients and research institutions have access to and can trust each other's data by using zero-knowledge proof to check if patients' medical records are up to snuff without compromising patients' privacy and by using proxy re-encryption technology to make sure that researchers can decipher the intermediate ciphertext. Patients and research institutions can conduct transactions according to predefined terms using this concept, which can also execute distributed consensus based on the PBFT algorithm. Through theoretical analysis and performance assessment, it has been shown that the suggested scheme is both practical and efficient compared to other usual schemes. It also satisfies security and privacy needs including confidentiality, integrity, and availability.

As more versatile communication services are offered, Xinyin Xiang et al. [11] suggested a novel method that raises privacy and security issues. While ensuring the security of e-health systems, it is an intriguing topic to provide effective authentication of medical data for diverse users. This study introduces a strategy for e-health identity management and user authentication (PBBIMUA) that is permissioned and built on the blockchain. Medical data has very specific security needs, and our approach meets all of them. Performance is better than existing techniques according to assessment and security analysis, which focuses on lightweight construction and reduced network latency with strong security requirements. It is clear from the experiments that the system is quite efficient.

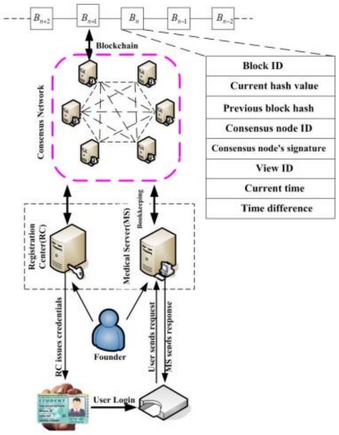


Fig.2 Block chain network model [6]

A Blockchain-based approach to provide a holistic solution was suggested by Mohamed Younis et al. [12]. Healthcare organisations and providers can easily comply with privacy rules with our solution, which puts patients in control of giving and removing access rights. Blockchain will keep track of sessions and access controls, while cloud storage will save the sensor data. Furthermore, a new secure communication protocol and data-driven authentication mechanism is suggested to lessen the possibility of fraud and identity theft. To implement this standard, smart contracts govern all communications between the cloud, patients, and healthcare practitioners. Utilising AVISPA, the security features of the proposed approach is accessed and demonstrate its computing efficiency.

Key Management, Authentication, Data-Driven Secure Communication, Smart Healthcare, and Blockchain are Index Terms.

According to Arun Sekar Rajasekaran et al. [13], an anonymous authentication mechanism based on blockchain technology is used to protect the privacy and anonymity of the end-users, who are the doctor or patient. Additionally, end-users conduct mutual authentication in this work before encrypting and decrypting confidential data. Better performance analysis is also achieved by implementing a transfer authentication mechanism between doctors so that patients are not re-authenticated every time they go from one doctor to another. The proposed work's resilience against several types of attack is shown in the security analysis section. Lastly, compared to analogous works that have been performed before, the suggested work's performance study shows that computational and communication expenses are reduced.

To provide complete privacy preservation and quick ciphertext retrieval for EMRs, Jingwei Liu et al. [14] suggested a blockchain-based inner product searchable encryption system with multi-keyword search (MK-IPSE). Not only does inner product encryption (IPE) provide access policy concealment, but it can also set access rights so that only users with specified characteristics can receive the target files. In addition, the suggested method applies robust and efficient multi-keyword search by integrating searchable encryption (SE) with federated blockchain (FB). When it comes to compute and storage, MKIPSE outperforms the current systems. Security testing has also shown that our approach is impervious to IND-CKA and collaboration assaults.

A new paradigm for electronic health records (EHRs) is being developed by Fei Tang et al. [15] to address the core issue with cloud-based EHRs. As a remedy, integrating the new blockchain technology is proposed into EHRs, which will be referred to as blockchain-based EHRs for simplicity. Using a consortium blockchain as an example, the system paradigm of blockchain-based EHRs is explicitly described. Furthermore, electronic health records (EHRs) place a premium on the authentication problem. On the other hand, there are limitations to the current authentication methods used for EHRs built on the blockchain. This study also includes a proposal for an authentication mechanism for electronic health records (EHRs) built on the blockchain. An identity-based signature method is provided that utilizes multiple authorities and is capable of withstanding a collusion assault using N out of N −1 authorities. Additionally, our system outperforms current blockchain-based EHR authentication systems in terms of efficiency in both signature and verification algorithms, and it is provably safe in the random oracle model.

Summary

1. The rapid growth and varied nature of IoMT have made safeguarding it a formidable obstacle, as new security threats emerge and old ones get worse.

2. If there was no proof-of-work (PoW) on a blockchain network, a malicious user might theoretically launch a denial-of-service (DoS) assault by flooding the network with blocks.

3. The primary concern with data transmission across networks is data security. Internet of Medical Things (IoMT) apps and platforms are vulnerable to security breaches since they rely on a central cloud.

4. Using only the blockchain idea Secure files have not made use of any new algorithms. We need to implement additional algorithms to safeguard our hospital data.

III. PROPOSED SYSTEM

The primary concern with data transmission across networks is data security. Internet of Medical Things (IoMT) apps and platforms are vulnerable to security breaches since they rely on a central cloud. Concurrently, the system is launched with a smaller number of nodes, which facilitates the use and development of blockchain technology in healthcare data. Consensus and block creation are two uses for the alliance medical blockchain system's medical chain. Data integrity, privacy, and nonrepudiation can be achieved with identity-based encryption and electronic signature technologies. Because all nodes are contributing data, cyberspace is more open and behaviour can be more easily tracked. The data certification and contract signing procedure is finished and fully compliant. Both the hash and encoding algorithms are customisable, allowing users to choose between SHA-256 and BASE64. Multiple blockchain systems have confirmed its dependability. uses the contents of the block header in conjunction with a SHA-256 hash operation to produce a hash value. When a miner's hash value drops below a certain level, it means they've successfully mined and are ready to broadcast a block to the whole network.We're making use of both algorithms. File storage of medical data makes use of the key IDE technique, while the SHA algorithm is used to avoid passwords. For that reason, this research takes into account SHA-256 and IDE for producing block hashes.

3.1. Existing System

A variety of approaches to securing IoMT have been proposed by many authors. Protecting sensitive information during IoMT can be as simple as encrypting it. The initial communication, known as "plain text," was encrypted into "cipher-text" using encryption methods. The public channel is used to send the cipher-text to the recipient. The recipient is thereafter responsible for decrypting the communication. Data encryption can be accomplished in several ways. A lightweight end-to-end key management technique is implemented in response to resource constraints and privacy concerns. plan that relies on cloud computing and Internet of Things (IoT) sensors to keep tabs on other private data, including that which is associated with digital signatures, time stamp mechanisms, and asymmetric technologies. When it comes to delivering medical treatments, this approach is very efficient while using minimal medical resources. A secure authentication and key agreement was suggested by Li et al. Because it includes private and sensitive information, a patient's medical record can be accessed by anybody, including potential assailants or those seeking vengeance. The transmission of such data would be secure and encrypted. Due of the massive volume of medical information, IoMT devices need massive storage infrastructure for real-time processing. These electronic medical records are crucial for providing the best care for the patient and are kept private. Electronic medical reports (EMRs)

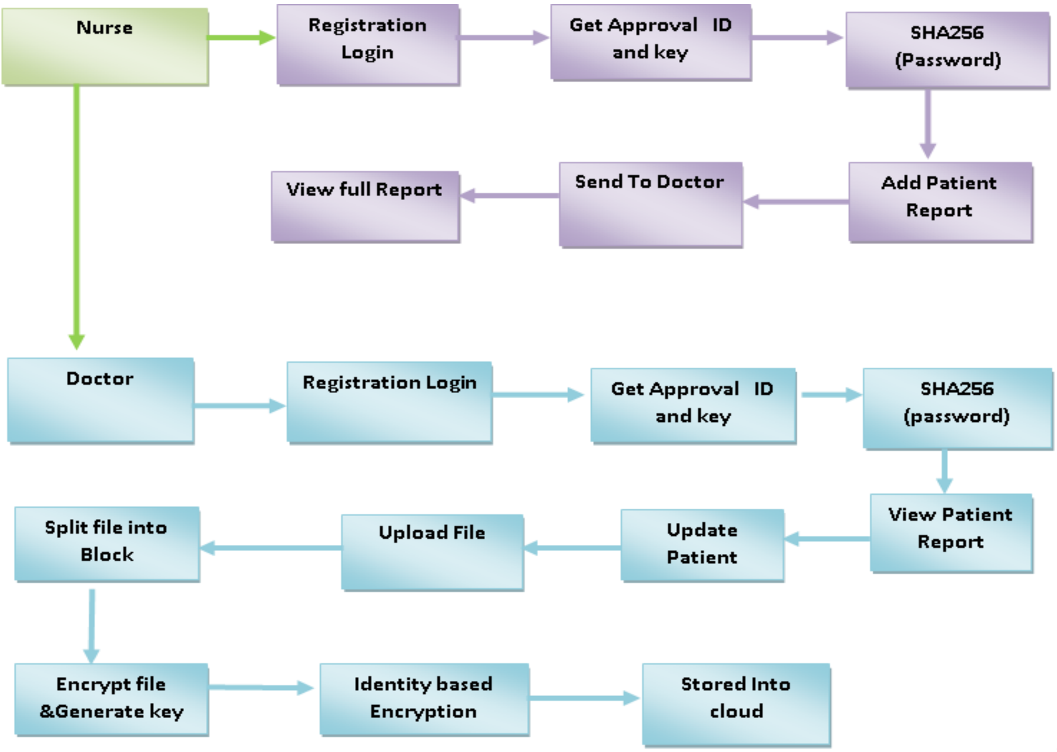


Fig.3 Architecture of the proposed model (Hospital Part)

3.2. System module

In this work, a blockchain-based healthcare management system is provided that is modular in design and aims to facilitate secure and private data exchange among administrators, nurses, patients, and doctors. The system uses the IDE encryption method to protect doctor data, has administrator permission, and encrypts passwords with SHA-256 for access control. By using the blockchain, patients can be certain that their medical records will remain private and uncompromised. With the administrator's OK, doctors can view patients' medical records. Using the IDE encryption method, doctors can protect their patients' private medical records. In order to maintain continuity of treatment, nurses work under the supervision of doctors and access patient information. Transparency and accountability in patient care are guaranteed by this. System operations, including user approvals and security measure enforcement, are overseen by administrators. Furthermore, the blockchain records administrator interventions, creating an indelible audit trail that ensures accountability.

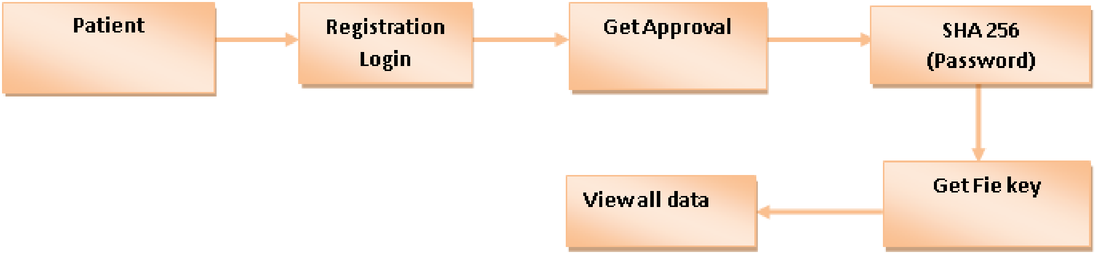


Fig.4 Architecture of proposed model (Patient part)

3.3. Blockchain model

A healthcare data management system based on the blockchain concept that is designed to improve the safety, openness, and effectiveness of healthcare data interchange and administration for everyone involved, including patients, doctors, nurses, and administrators. With blockchain technology, the system can accommodate the many moving parts of the healthcare ecosystem while guaranteeing the authenticity, immutability, and accessibility of data. Healthcare providers can access accurate and current information to give prompt and personalised treatment, while patients have more control over their health data. Facilitating confidence and cooperation in the healthcare ecosystem, administrators can simplify data management procedures while guaranteeing compliance with privacy laws. They take patient vitals, give out treatments, and coordinate care with other medical staff via the blockchain network. Patient information is safeguarded from unauthorised access by means of the system's encryption and access restrictions.

3.3.1. SHA-256 Model

Secure storage of medical report passwords and generation of authorization keys are both made possible by the SHA-256 algorithm. Here is one way to put it into action:

Storing Passwords:

The SHA-256 technique should be used to hash passwords when they are established by users (e.g., doctors, nurses, and patients).The system's database subsequently stores the hashed password. If you want to take security seriously, you should only save hashed passwords and not the actual passwords themselves. For authentication purposes, the user's password is hashed using SHA-256 when they log in. This hash is then compared to the one saved in the database.

The SHA-256 algorithm is fundamental to blockchain technology in many ways, but especially when it comes to mining and generating safe, immutable blocks.

- Input data and generate SHA constant.
- Preprocessing the database
- A hash of the preceding block, a timestamp, transaction data, and a nonce are all parts of the information that each block's header carries.
- Transactions are aggregated into blocks by miners, who then compete to discover a nonce value that, when added to the other data included in the block header, produces a hash value that satisfies certain requirements.
- Until a good hash is obtained, miners will continually use the SHA-256 algorithm to hash the contents in the block header, including the nonce.
- Concatenation of blocks
- Padding with zeros or ones for 512 sequence generation.
- The SHA-256 hash function is used to generate this hash, ensuring that any change to the block's contents or order of transactions would result in a completely different hash value.
- IN MD construction compression function
- Concatenation of hashes and values.
- Append and iterative compress the values
- Appending hashing value output

Generating approval key

To construct a secure authorization token, one can combine different data pieces and hash them using SHA-256. This process produces an approval key. To make sure it's unique and avoid replay attacks, the approval key might comprise information like the user ID, timestamp, and a random nonce. For permission reasons, the requester receives the approval key once it has been produced.

3.3.2. Identity-Based Encryption (IBE) model

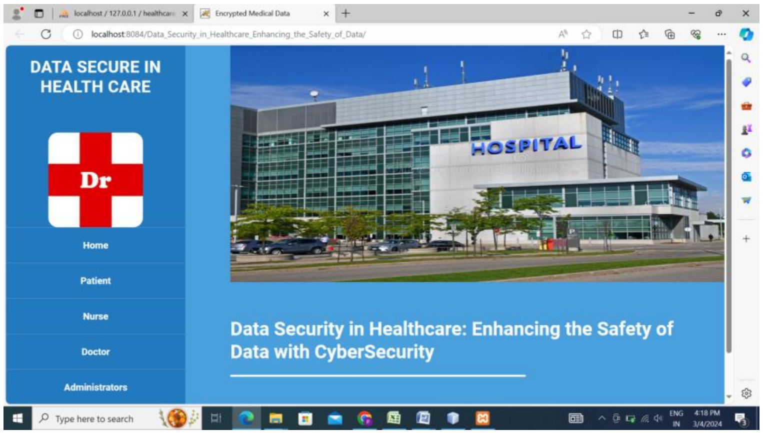
Encrypting patient report data using Identity-Based Encryption (IBE) makes it easy to ensure that only authorised individuals can access and decode the data. Using Drive HQ or another cloud storage provider as an example, here is how to use IBE to encrypt patient report data. In order to set up an IBE system, you must have a trusted authority (TA) that uses user identities (such email addresses) to produce private keys. A master private key and matching master public parameters are generated by the TA. Every user, who is usually a doctor is given a distinct identification, which is usually their email address. Upon doctor registration, the TA receives the email address, uses it to build a private key verifying the doctor's identity, and then securely sends the key to the patient. In order to encrypt a patient report, a doctor has to know both the patient's and their own identities in order to create a public key the doctor uploaded data encrypted to the cloud. Provide the doctor with the patient's access key so they can see the report whenever the patient requests it.

IV. RESULT AND DISCUSSION

In this healthcare system, everyone from patients to doctors to nurses must first register and have administrator clearance before they can use the platform. Their passwords are saved securely using the SHA-256 approach, which guarantees strong authentication encryption. In order for doctors to access patient records, nurses are using the platform to submit the necessary paperwork.The doctor will use the ide encryption model to upload the patient's solution and report to the drive/hq cloud. A private key is created in order to decode the information. Administrator will send the file download link to the patient's email. Also, the blockchain records administrator interventions, so there's an unchangeable record of who did what. Patient information is safeguarded from unwanted access by means of the system's encryption capabilities and access restrictions.

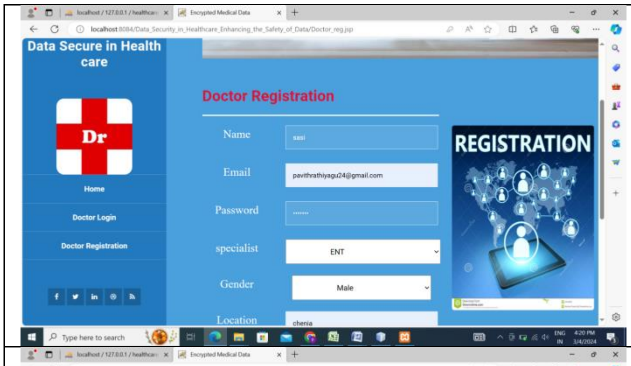
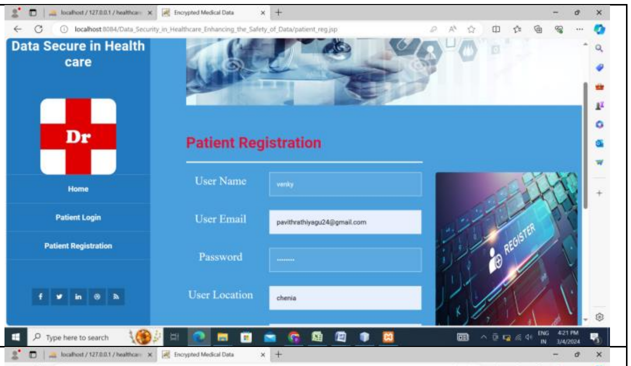
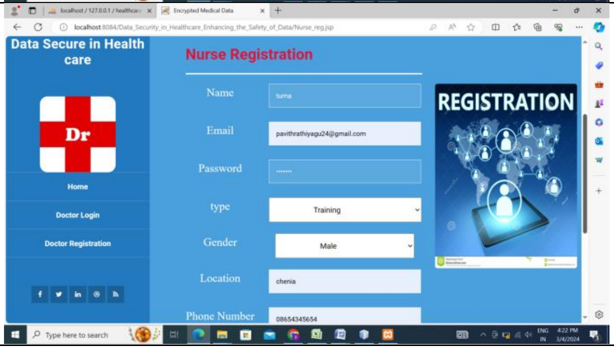
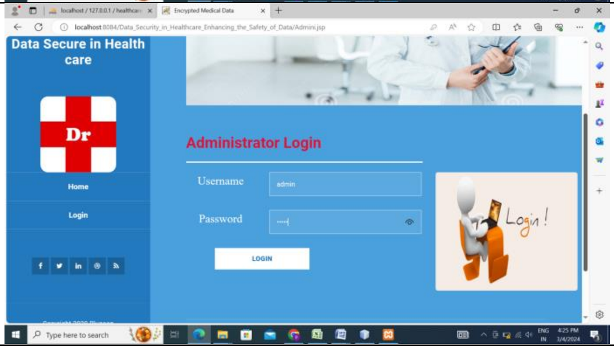
Home screen of the Application

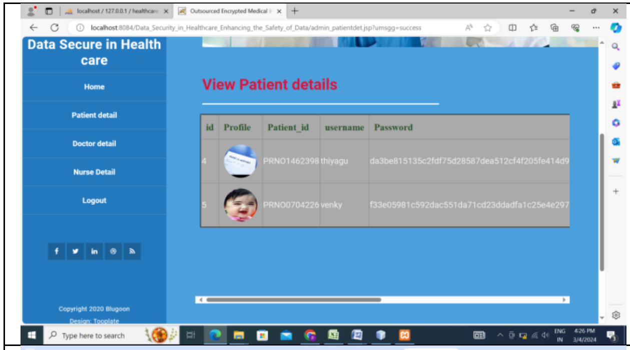
Table I. Process flow of the proposed model



localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/

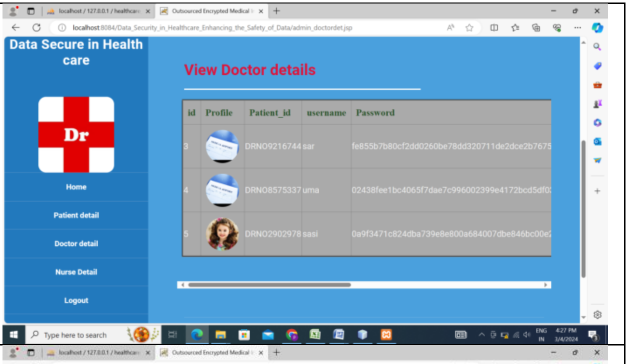
Data Security in Healthcare: Enhancing the Safety of Data with CyberSecurity

 localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/Doctor_reg.jsp Data Secure in Health care Home Doctor Login Doctor Registration Doctor Registration Name: sasi Email: pavithrathiyagu24@gmail.com Password: .... specialist: ENT Gender: Male Location: chenia REGISTRATION	 localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/patient_reg.jsp Data Secure in Health care Home Patient Login Patient Registration Patient Registration User Name: venky User Email: pavithrathiyagu24@gmail.com Password: .... User Location: chenia REGISTER
 localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/Nurse_reg.jsp Data Secure in Health care Home Doctor Login Doctor Registration Nurse Registration Name: tuma Email: pavithrathiyagu24@gmail.com Password: .... type: Training Gender: Male Location: chenia Phone Number: 08654345654 REGISTRATION	 localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/Admini.jsp Data Secure in Health care Home Login Administrator Login Username: admin Password: .... LOGIN Login !


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/admin_patientdet.jsp?umsgg=success
Data Secure in Health care
Home
Patient detail
Doctor detail
Nurse Detail
Logout
Copyright 2020 Blugoon
Design: Tooplate

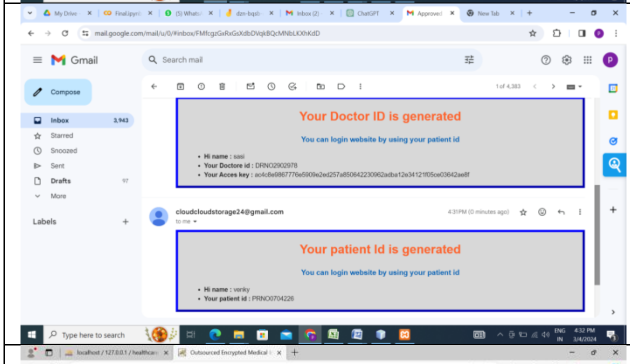
View Patient details

id	Profile	Patient_id	username	Password
4		PRNO1462398	thiyagu	da3be815135c2fdf75d28587dea512cf4f205fe414d9
5		PRNO0704226	venky	f33e05981c592dac551da71cd23ddadfa1c25e4e297


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/admin_doctordet.jsp
Data Secure in Health care
Dr
Home
Patient detail
Doctor detail
Nurse Detail
Logout

View Doctor details

id	Profile	Patient_id	username	Password
3		DRNO9216744	sar	fe855b7b80cf2dd0260be78dd320711de2dce2b7675
4		DRNO8575337	uma	02438fee1bc4065f7dae7c996002399e4172bcd5df0
5		DRNO2902978	sasi	0a9f3471c824dba739e8e800a684007dbe846bc00e



Your Doctor ID is generated

You can login website by using your patient id

- Hi name : sasi
- Your Doctore id : DRNO2902978
- Your Acces key : ac4c8e9867776e5909e2ed257a850642230962adba12e34121f05ce03642ae8f

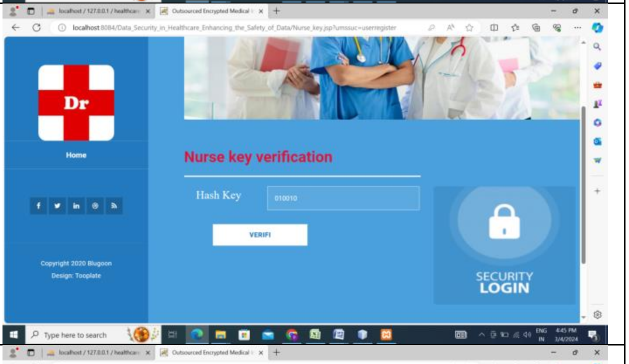
cloudcloudstorage24@gmail.com
to me

4:31 PM (0 minutes ago)

Your patient Id is generated

You can login website by using your patient id

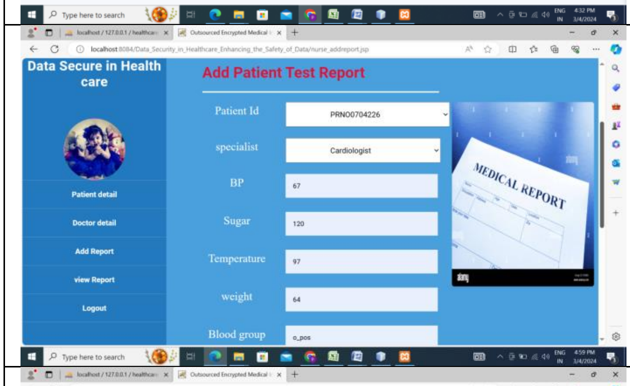
- Hi name : venky
- Your patient id : PRNO0704226


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/Nurse_key.jsp?umssuc=userregister
Dr
Home
Copyright 2020 Blugoon
Design: Tooplate
SECURITY LOGIN

Nurse key verification

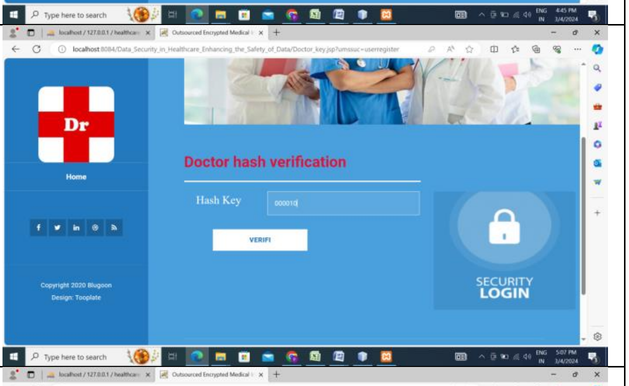
Hash Key: 010010

VERIFI


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/nurse_addreport.jsp
Data Secure in Health care
Patient detail
Doctor detail
Add Report
view Report
Logout
MEDICAL REPORT

Add Patient Test Report

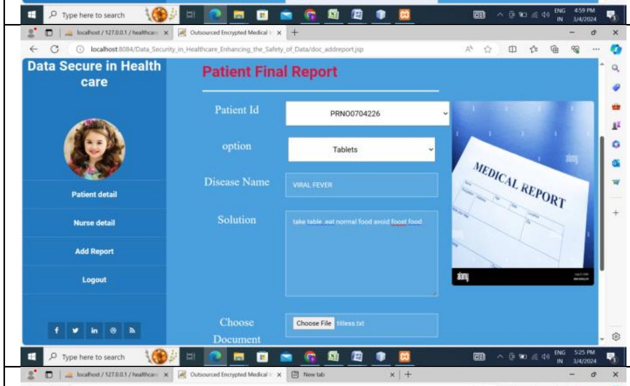
Patient Id	PRNO0704226
specialist	Cardiologist
BP	67
Sugar	120
Temperature	97
weight	64
Blood group	o_pos


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/Doctor_key.jsp?umssuc=userregister
Dr
Home
Copyright 2020 Blugoon
Design: Tooplate
SECURITY LOGIN

Doctor hash verification

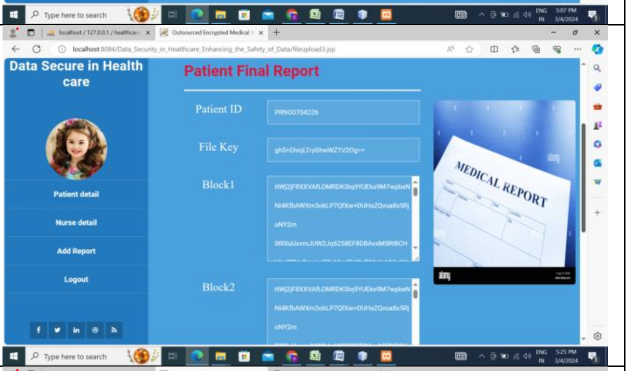
Hash Key: 000010

VERIFI


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/doc_addreport.jsp
Data Secure in Health care
Patient detail
Nurse detail
Add Report
Logout
MEDICAL REPORT

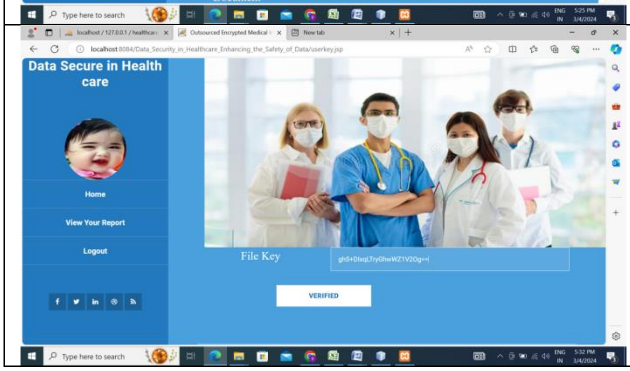
Patient Final Report

Patient Id	PRNO0704226
option	Tablets
Disease Name	VIRAL FEVER
Solution	take table ,eat normal food avoid fooat food
Choose Document	Choose File titless.txt


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/fileupload3.jsp
Data Secure in Health care
Patient detail
Nurse detail
Add Report
Logout
MEDICAL REPORT

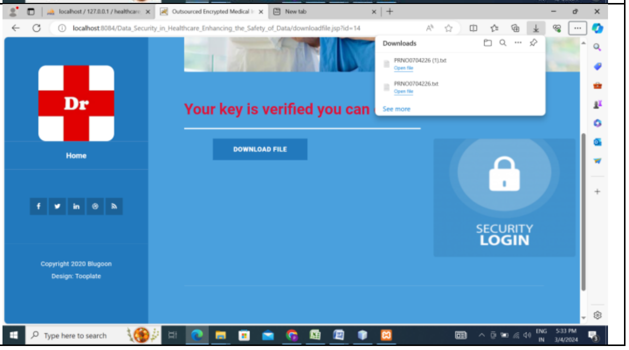
Patient Final Report

Patient ID	PRNO0704226
File Key	ghS+DlxqLTryGhwWZ1V2Og==
Block1	ttWj2jF8XXVAfLOMRDKStq9YUEks9M7wpbeN NI4KfbAWXm3okLP7QfXw+DUHsZQvua8x5Rj oNY2m 0RlXuUxvmJUW2Jq6258EFBDBAvxM5RtBCH
Block2	ttWj2jF8XXVAfLOMRDKStq9YUEks9M7wpbeN NI4KfbAWXm3okLP7QfXw+DUHsZQvua8x5Rj oNY2m


localhost:8084/Data_Security_in_Healthcare_Enhancing_the_Safety_of_Data/userkey.jsp
Data Secure in Health care
Home
View Your Report
Logout

File Key: ghS+DlxqLTryGhwWZ1V2Og==

VERIFIED



Your key is verified you can

DOWNLOAD FILE

The following steps make up the suggested system: To get access to the app, doctors must first register, followed by patients and nurses. The central administrator has authorised all registered users. A central administrator has the ability to review and authorise all users, as well as examine the information of registered patients, doctors, and nurses. Every user gets an ID based on their work after it's authorised, and those IDs are sent to the right people. Patients' medical records can be uploaded by the nurse. Following the administrator's upload to the cloud, the document is reviewed by the doctor for verification. Block chain is now being used. The papers are encrypted and then stored in the cloud after being divided into chunks. Both the nurse and the patient get an email with the decryption key. They can access the decrypted document by downloading it, but only after entering the key.

Advantages of the proposed model

The main benefit is the increased accessibility and quality of healthcare treatments throughout the whole network. Nevertheless, there is still opportunity for growth in tackling different security concerns, even with these advantages.

The data is safer and more trustworthy, with less chance of data loss and theft. At the same time as it authenticates and authorises users, the Consensus algorithm and hash algorithms keep data intact.

Ensuring data reliability and security by preventing unauthorised access and loss of data. In addition to authenticating and authorising users, the Consensus algorithm and hash algorithms ensure that data remains intact.

Health care records will be more efficient because to the two algorithms that are applied, SHA and IDE, which will prevent data attackers.

V. CONCLUSION

Using the SHA-256 paradigm for password encryption, the healthcare system guarantees a safe registration procedure for patients, doctors, and nurses. When doctors get patient reports from nurses, they encrypt them using IDEA and then save them to the cloud. Through a blockchain paradigm, patients are granted private keys by their doctors, which allow them safe access to their medical information. Not only does this unified method encourage privacy and security of patient information, but it also makes it easier for medical staff to work together effectively. Patients are more empowered and have more faith in healthcare providers because of the system's strong security features, which include encryption and blockchain technology. It helps create a more interconnected healthcare environment and improves patient outcomes via its openness and efficiency.

REFERENCES

[1]. Vatambeti, R., Krishna, E. P., Karthik, M. G., &Damera, V. K. (2023). Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things. *Cluster Computing*, 1-13.

[2]. Alsuqaih, H. N., Hamdan, W., Elmessiry, H., &Abulkasim, H. (2023). An efficient privacy-preserving control mechanism based on blockchain for E-health applications. *Alexandria Engineering Journal*, *73*, 159-172.

[3]. Miao, J., Wang, Z., Wu, Z., Ning, X., & Tiwari, P. (2024). A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Systems with Applications*, *237*, 121329.

[4]. Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A review of Blockchain-based secure sharing of healthcare data. *Applied Sciences*, *12*(15), 7912.

[5]. Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.

[6]. Egala, B. S., Pradhan, A. K., Badarla, V., &Mohanty, S. P. (2021). Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet of Things Journal*, *8*(14), 11717-11731.

[7]. Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ...&Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable

encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.

[8]. Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., &Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors*, *22*(2), 528.

[9]. Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C., &Mumtaz, S. (2023). Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. *IEEE Internet of Things Journal*.

[10]. Huang, H., Zhu, P., Xiao, F., Sun, X., & Huang, Q. (2020). A blockchain-based scheme for privacy-preserving and secure sharing of medical data. *Computers & Security*, *99*, 102010.

[11]. Xiang, X., Wang, M., & Fan, W. (2020). A permissioned blockchain-based identity management and user authentication scheme for e-health systems. *IEEE access*, *8*, 171771-171783.

[12]. Younis, M., Lalouani, W., Lasla, N., Emokpae, L., & Abdallah, M. (2021). Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access. *IEEE Systems Journal*, *16*(3), 3746-3757.

[13]. Rajasekaran, A. S., &Azees, M. (2022). An anonymous blockchain-based authentication scheme for secure healthcare applications. *Security and Communication Networks*, *2022*, 1-12.

[14]. Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C., &Mumtaz, S. (2023). Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. *IEEE Internet of Things Journal*.

[15]. Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An efficient authentication scheme for blockchain-based electronic health records. *IEEE access*, *7*, 41678-41689.