Secure Healthcare System Using Blockchain With Insurance Processing

Satheesh Kumar M
Dept of Computer Science and Engineering
Mount Zion College of Engineering and Technology
Pudukkottai

Abstract- *The patient's medication information and health history are stored in Electronic Health Records. Because it contains valuable records, health information attracts the attention of attackers. The loss of electronic health records results in the administration of incorrect medication or surgery.Healthcare systems provide fewer security procedures to protect patient information. Traditional electronic health records (EHRs) manage medical information one at a time with the assistance of specific hospitals, resulting in the inconvenient sharing of records.The difficulty of fact sharing in traditional EHRs is solved by cloud-based EHRs. However, cloud-based EHRs have a centralized problem in the form of a cloud service centre and key-generation centre.The proposed effort focuses on developing a new EHRs paradigm that can aid in dealing with the centralized issue of cloud-based EHRs.The solution is to apply the nascent blockchain technology to EHRs (denoted as blockchain-based EHRs for convenience). First, define the system model of blockchain-based EHRs in a blockchain scenario. Furthermore, the authentication issue may be critical for EHRs. Current authentication techniques for blockchain-based EHRs, on the other hand, have their own vulnerable issues. In addition, an authentication strategy for blockchain-based EHRs is proposed here. Our solution is a role-based signature scheme with multiple authorities that can withstand a collusion attack.Furthermore, in the random oracle model, the proposed technique is probably safe and provides more efficient signature and verification procedures than existing authentication schemes. This suggested project also focuses on the insurance claim process for patients. It assists patients in obtaining insurance from the approved insurance industry.*

Keywords- EHR Sharing,Blockchain Implementation, Authentication Verification, Data Distribution, Insurance Claiming.

I. INTRODUCTION

Access control is a security method that governs who or what can view or utilize resources in a computing environment. It is a fundamental idea in security that reduces risk to the firm or organization.Access control can be split into two categories physical and logical. Physical manipulation restricts access to campuses, buildings, rooms, and physical IT property. Connections to computer networks, files, and data are restricted by logical access control.Access control structures identify, authenticate, and permit customers and entities by evaluating needed login credentials, which may include passwords; personal identification numbers (PINs), biometric scans, security tokens, or other authentication elements.Multifactor authentication necessitates extra authentication factors and is frequently used as part of layered defense to defend access to manipulating systems. Access control is intended to decrease the threat of unauthorized access to physical and logical entities.Access control is a basic component of security compliance programs that ensures security technology and access control policies protect private records, including client information.Many firms have recently implemented infrastructure that restricts access to networks, computer systems, packages, files, and sensitive information, such as individually identifiable data and intellectual data access.Access control structures are complicated and can be difficult to manipulate in dynamic IT environments that contain on-premises structures and cloud services. After some excessive-profile breaches, technology vendors have shifted faraway from single sign-on structures to unified access control, which offers access controls for on-premises and cloud environments.

1.1 BENEFITS OF ACCESS CONTROL

In recent years, there has been a boom in interest in cloud-based access to content, drawing organizations of all sizes and across industries. That comes as no surprise to anyone who has seen the benefits of cloud-based solutions.

From simplified system administration to pricing flexibility, cloud-primarily based access manipulates provide some very interesting characteristics when compared to traditional, on-premise structures. Some notable instances are provided below.

1.1.1 Accessibility from anywhere with an Internet connection

While some traditional access control systems support remote connectivity, cloud systems are built with mobile accessibility in mind. Authorized users can examine or manage device interest by logging into the relevant access to control app, online portal, or network.Aside from convenience, this allows users to receive alerts and take action in the event of a crisis or emergency.

1.1.2 Flexible cost management

Whereas traditional access control systems usually have expensive upfront installation and equipment expenses, cloud-based services provide far more price options.Instead of purchasing online equipment altogether, consumers can lease it from an authorized reseller, avoiding large capital investment charges in exchange for low continuing operational costs.

1.1.3 Reduced burden on user staff

Maintaining a company service, especially one as important as access control, takes time and work. Customers can significantly reduce the burden on their own IT workers by outsourcing the hosting and maintenance of on-site PCs, servers, data-redundancy infrastructure, and associated processes to the integrator.A cloud-based solution can reduce the strain of IT participation by 97%, depending on the software. If the consumer prefers, management of cloud services can be delegated partially or entirely to the integrator.

1.1.4 System reliability

Keeping all records on a website might be a dangerous task: Unless the individual has strong precautions in place, an energy surge or network failure can disrupt service operation or result in data deletion.To maintain the safety and integrity of the cloud service and information, cloud-based access control solutions typically use centralized data centre that are established with efficient backup energy and storage systems.

1.1.5 Round-the-clock updates and monitoring

Software updates and patches are essential for keeping the access control system up to date and addressing any vulnerability. These upgrades, however, are only advantageous if they are implemented on time.Updates can be put out quickly and concurrently across machine devices with cloud-based access to manage systems, rather than requiring staff to handle them.This improves device performance and security while decreasing the possibility of human error. Furthermore, many cloud-based solutions provide 24/7 monitoring services, assisting to improve response time, provide piece of mind, and free up stop person employees to address other pressing business concerns.

Cloud-based solutions, like traditional access control systems, differ each commercial enterprise, as do the features that consumer's value the most. Perhaps the most exciting benefit is that customers can discover new ways to not only increase facility security, but also enhance IT and other commercial enterprise-wide operations.

1.2 MEDICAL DATA SHARING IN CLOUD

Traditionally, medical data was recorded on paper, which was easily damaged and altered. As a result, the data had to be saved electronically. However, the medical database could be manipulated with or permanently deleted.The restriction of information was also a worry. When a person or other entity, such as someone with or without intent, accesses information that shouldn't have been seen without the patient or hospital's consent, information blocking happens.When it comes to improving quality or addressing problems like resource allocation and information blocking, technology always plays a major role. In the case of medical care, data exchange technology has to develop through timePatients typically have access to a wide range of healthcare professionals, such as general practitioners, specialists, and even therapists. They all need to safely communicate health records without any modification because one condition may result from another.If all data is securely saved and exchanged, the patient does not need to be a professional or have a good memory to retain all of the data appropriately. Patients must keep their medical data history up to date. Furthermore, transferring data on paper or even by email has time, speed, storage, and security implications. Data storage in a database has various restrictions, including limited storage space and vulnerability to cyber-attacks. Attackers may get access to the system and obtain sensitive patient data. A centralized database cannot be relied on because varied access rules for different users, searching across an encrypted channel, big memory for medical data storage, and so on.As a result, researchers developed a block chain-based solution for medical healthcare that will not only safeguard data from tampering but will also prevent data leakage.This technique has the potential to preserve data and thus ensure dependability. And, when combined with cloud computing technologies, storage issues can be eliminated because the cloud is trusted for storing and managing data.Furthermore, block chain can handle cloud security challenges. Indeed, medical data sharing and storage on a Block chain-based cloud can handle a variety of medical data issues.

II. RELATED WORK

Guo, et.al,.[1Present a multiple-authority attribute-based signature technique where a patient attests to a message based on the attribute without revealing anything other than the proof that he did so.Furthermore, there are various authority without a trusted single or central one to generate and distribute the patient's public/private keys, which eliminates the escrow problem and corresponds to the block chain's style of distributed data storage.This protocol prevents collusion attacks from corrupted authorities by exchanging the secret pseudorandom function seeds across authorities. We further formally establish that, in terms of the attribute-enforceability signer's and perfect privacy, this attribute-based signature method is secure in the random oracle model under the assumption of the computational bilinear Diffie-Hellman.EHRs systems can be administered collaboratively assuming that there is a EHRs system in a cloud storage platform that comprises of some departments, including hospitals, pharmaceutical departments, insurance departments, illness research departments, and so forth. To prevent the misuse of EHRs, all departments may provide services to patients jointly while imposing restrictions on their respective rights.

Dagher, et.al,.[2 To ensure the protection of patients' sensitive information, suggest a block chain-based architecture for safe, effective access to medical records for patients, providers, and other stakeholders. Consensus, Classification, Service History, Ownership, Permissions, and Re-encryption are six distinct types of smart contracts that are used by our suggested framework, Ancile, to operate.We enable patients to benefit from enhanced utility while minimizing the need to interact with each contract by using six different contracts. This increases the efficiency of the patient experience while decreasing privacy risks.We use the contracts to generate further contracts to achieve a high level of separation. As a result, the patient may be the only node that is explicitly told the location of their information.Ancile uses smart contracts to keep cryptographic hashes of stored records and query links, ensuring the integrity of EHR Databases. By employing a smart contract to govern access control, patients may also see and control who has access to their confidential information.Furthermore, patients can provide transfer permissions to other nodes. This is made possible by using identity-checking to authenticate who has access to records, as well as proxy re-encryption to prevent having to re-encrypt the record for each transmission.

Mehmood, et.al,.[3] Propose a system that protects users of health care apps from adversaries and the authentication server by providing complete privacy and anonymity.The fundamental purpose of this study is to enable anonymous authentication to provide identity privacy for smart cloud-based healthcare apps.The proposed technique is broadly applicable and can be used for various cloud-based applications. In some cases, the activities performed on a specific set of data over time can potentially identify the user.As a result, the proposed technique is best suited for instances in which the exact user cannot be recognized through data operations. Other challenges, such as location privacy and query privacy in smart health applications, are also essential.Patients can use their smartphones to make an appointment with a healthcare practitioner or call an ambulance in an emergency without revealing their identity.

Wang, et.al,.[4] Make a proposal for a cloud-based EHR system that employs an attribute-based crypto system and blockchain technology. We use ABE and IBE to encrypt data in this system, guaranteeing fine-grained access control for encrypted data, and IBS to perform digital signatures.We offer a new cryptographic primitive termed combined attribute-based/identity-based encryption and signature (C-AB/IB-ES) to perform different functions of attribute-based encryption (ABE), identity-based encryption (IBE), and identity-based signature (IBS) in a single cryptosystem. This considerably simplifies system management and eliminates the need to implement various cryptographic systems for different security requirements.Furthermore, we use blockchain technology to ensure that medical data cannot be altered with and that the data sources can be traced.Finally, we provide a demo application for the medical insurance scene.In this approach, patients allow their data access policy to the hospital (with their signature) based on their actual requirement, and then send the signed authorization letters to the blockchain data pool to await consensus node processing.

Sun, et.al,.[5] In order to securely share EHR data with many CDOs, suggest a blockchain-based EHR data storage system using a productive on-chain and off-chain cooperation storage approach.Our blockchain-based storage system offers the following benefits: (1) Implementing secure EHR data exchange between several CDOs using blockchain such that the stored and shared EHR data are unaltered, unforgeable, and verifiable. (2) Use a combination of on-chain and off-chain storage to achieve distributed and large-scale secure EHR data sharing. Each transaction on the blockchain contains the address of a single EHR data record, and each node off the block chain stores the actual EHR data. This overcomes the blocks' storage restriction while making it simpler for users to find each piece of EHR data. The proposed DABS verification protocol should also be subjected to a rigorous security study to determine its unforgeability, security from collusion attacks, anonymity, and non-

repudiation. Our experimental analysis shows that the suggested DABS method is efficient and simple to implement.

III. EXISTING METHODOLOGIES

All medically relevant information is digitalized and kept on the hospital's server in EHRs. When a patient returns to the hospital, he or she can search past information, including the patient's and doctor's names, the date, the diagnosis, and other details.EHRs have received a lot of attention since they have a significant applicability in the medical industry. The current system is working to develop a new EHR paradigm that will aid in resolving issues with cloud-based EHRs.Utilizing the cutting-edge blockchain technology is the answer. In general, blockchain can be compared to a distributed, decentralized database. Traditional network architectures and application systems, such KGC, cloud service providers, and others, have authority. A crucial component of blockchain-based EHRs is authentication. The data in blockchain-based EHRs must be authenticated, such as a doctor's diagnosis, unlike in the case of block chains, which are anonymous and lack an authentication mechanism for users.Therefore, create a reliable authentication system for EHRs that are blockchain-based. An identity-based signature system with multiple authorities (MA-IBS) that includes effective signing and verification algorithms and can fend against collusion attacks is an existing proposal.

IDENTITY BASED ENCRYPTION

By integrating extra functionalities of user revocation and ciphertext update simultaneously, the implementation of revocable-storage identity-based encryption (RS-IBE) enables the forward/backward security of ciphertext.

IBE

The issue of encryption key management is effectively tackled by Identity Based Encryption (IBE). IBE may safeguard data without the requirement for certificates by using any string as a public key. Any user can create a public key from a known identification value, such as an ASCII string, using identity-based systems.The Private Key Generator (PKG) that creates the matching private keys is an authorized third party. The master public key and associated master private key are first provided by the PKG.Any user can compute a public key matching the identity ID given the master public key by adding the master public key and the identity value. The user who is permitted to use the identity ID contacts the PKG to obtain a corresponding personal key, and the PKG generates the personal key for Identity ID using the master key.Users can thereby encrypt messages without first sharing keys with individual contributors. This is helpful when pre-distribution of authenticated keys is difficult or impossible because of technological limitations.The authorized person must, however, obtain the perfect personal key from the PKG in order to decode or sign messages.

RS-IBE

Confidentiality and backward secrecy can be provided by the non-revocable data exchange mechanism. Furthermore, the mechanism used to decrypt and re-encrypt all shared data can assure forward secrecy.This, however, introduces significant complications. It should be noted that the process of decryption and re-encryption inevitably involves users' secret key information, making the total data sharing system vulnerable to new assaults.In general, the effect of secret key should be limited to best common decryption, and it is not recommended to alter the cipher textual content on a regular basis using secret key.Efficiency presents still another difficulty. The data provider must often complete the download-decrypt-re-encrypt-upload operation in order to refresh the cipher text of the shared data.For cloud customers with limited computing and storage capacity, this approach is burdensome and unfavorable because it incurs high connection and compute costs.

IV. MEDICAL DATA SHARING USING BLOCKCHAIN WITH INSURANCE CLAIMING

Researchers proposed the idea of could base EHRs to address the issue of information sharing in the conventional EHRs. The use of cloud computing technologies in EHRs can be seen in cloud-based EHRs.There still has to be a cloud service provider acting as the system's authority in cloud-based EHR solutions. The cloud server will receive all medical-related data from the doctor, pharmacy, diagnostic lab, insurance provider, and so forth.Users can then use the cloud server to search for and download useful data. When multiple businesses use the same cloud server, they can conveniently share data.Next, when patients move from one hospital to another, the new hospital can access the patients' medical information via the cloud, negating the need for them to undergo additional medical testing.As a result, the issue of information sharing in conventional EHRs is resolved by cloud-based EHRs. Additionally, all data in cloud-based EHRs are only kept up to date by the authority, or cloud service provider; hospitals and other institutions can only tamper with the medically related data when they work together with the authority.

Only authorized users must have access to data stored in the Cloud in order for data sharing to be possible. The

consumers of blockchain-based EHRs are split into two categories in the proposed work.The EHRs server is at level 0, which is the lowest level. Medical insurance providers are found at level 2, which is represented by Level 1. All medical relevant data will be distributed and kept by all Level 1 users in blockchain-based EHR systems who can agree on the veracity of the shared data based on a particular process.Level 2 users are responsible for generating medical-related information, such as medical records from doctors and insurance policies from insurance agents.The decentralized nature of blockchain eliminates such reliance on authority. As a result, many individuals considered the uses of blockchain in various real-world scenarios, including EHRs, which we call blockchain-based EHRs.A suitable authorization procedure from Level 1 users to their patients can ensure the legitimacy of such information.The suggested framework restricts system access to certified users or stakeholders. The suggested blockchainbased infrastructure can track the activity of users. The sharing of patient data is validated using cryptographic procedures.The technology acts as a go-between for users and sensitive healthcare data. They presented a solution that employed a lightweight blockchain to ensure quick transactions and proper efficiency.As a result, cloud-based EHRs address the issue of information sharing in traditional EHRs. Furthermore, in cloud-based EHRs, all data are exclusively retained by the authority, i.e., the cloud service provider, and thus hospitals and other organizations can tamper with medical-related data only if they collaborate with the authority.

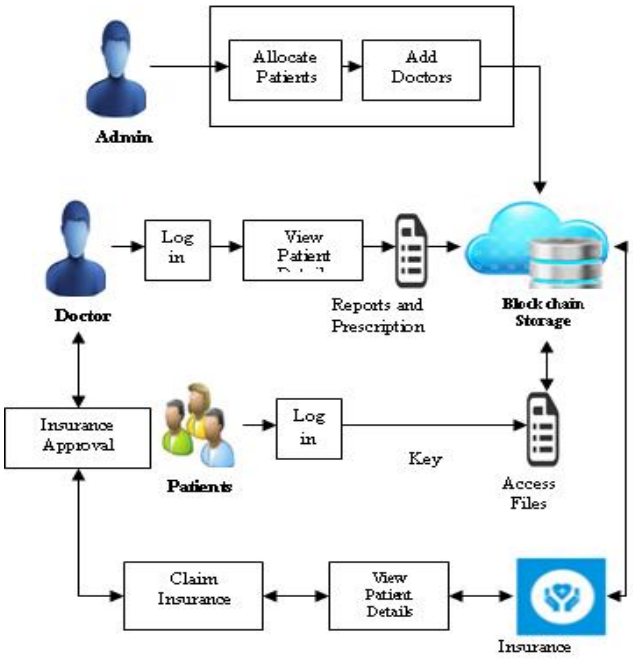


Fig 4.1: Architecture for Proposed Work

V. METHODOLOGY

Blockchain Technology

A blockchain is a digital notion that is used to store data. Because these blocks are connected together, their data is immutable. When a data block is linked to the other blocks, its data cannot be modified again. It will always be publicly accessible to everyone who wants to see it, just as it was when it was uploaded to the blockchain.

Because of the unique property of hash function that produces distinct outputs when given diverse inputs, the most widely used safe algorithms connected with blockchain technology are (SHA-1, SHA2, and SHA-256) encryption.Here, the hash function is a special key made to distinguish a transaction from a certain person in the petroleum supply chain.The blockchain technology is dependable for usage in a hashing crypto method that transforms bits of fixed-size data into character strings by generating an appropriate and robust hashing code.Each proposed transaction in a blockchain is hashed before being pushed into a block, and the hash pointers link each block to the following block to hold the previous hash data since it is irrefutable.As a result, any modifications to the hashing function used in blockchain transactions will produce a different hash string and have an impact on all the affected blocks.

Block and Hash Generation

1. A Block that includes details on current transactions.
2. Each piece of data produces a hash..
3. A hash is a combination of letters and integers.
4. The order in which transactions occurred is reflected in the database.
5. The hash depends on both the prior transaction's hash and the current transaction.
6. Any alteration to a transaction, no matter how slight, results in a brand-new hash.
7. The nodes examine the hash to ensure that a transaction has not been altered.
8. A transaction is included in a block if it receives the majority of nodes' approval.
9. The Blockchain is made up of individual blocks that each refer to one another.
10. A Blockchain works because it is replicated on numerous computers, each of which has access to it.

AES Encryption

The block cipher is another name for the AES cipher.On AES, no successful attacks have been documented. AES has benefits such as being simple to implement on processors with an 8-bit design and being effective when used on processors with a 32-bit architecture.Moreover, every action is transparent (e.g, XOR, permutation and substitution). AES encryption takes place across several cycles.Sub-byte, shift-row, mix-column, and add round key are the four main processes of a round. The substitution of bytes from a look-up table is known as sub-byte.The shifting of rows per byte length is known as shift row. Multiplication of the mix column over the Galois field matrix. Finally, the output matrix of the mix column is XORed with the round key in the add round key step.The size of the key affects how many rounds are required for encryption. These four stages are used for a 128-bit key in nine rounds, with the mix column step being ignored in the final round. Decryption is the opposite of encryption because all stages are recursive.

Algorithm Procedure

The Add round key stage is the first stage of the algorithm, which is followed by nine rounds of four stages and a tenth round of three stages.This holds true for both encryption and decryption, with the exception that the decryption algorithm is the opposite of the encryption method at each point of a round.These are the four phases:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The Mix Columns stage is simply skipped in the tenth round. The decryption algorithm's initial nine rounds are as follows:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

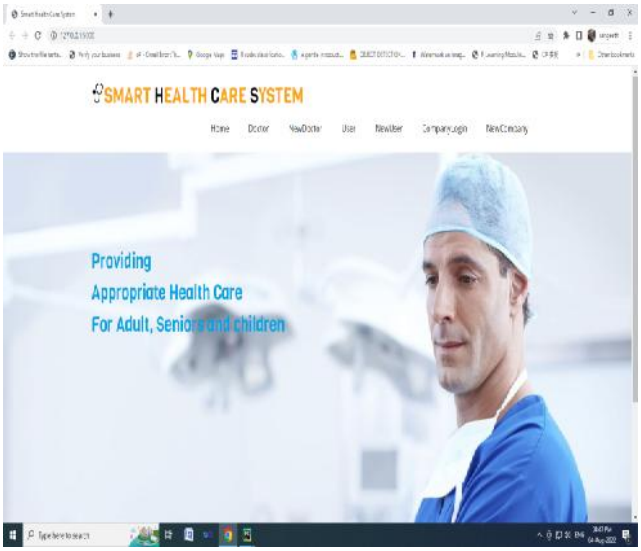
Again, the Inverse Mix Columns stage is just skipped in the eleventh round. We'll now take a closer look at each of these phases.

V. EXPERIMENTAL RESULTS

The effectiveness of the suggested system is demonstrated by the experimental results. Here, ASP.NET is used as the front end and SQL is used as the back end to develop access control based medical data exchange and insurance claim procedure. This will help to increase the security of files.

BLOCK CHAIN STORAGE

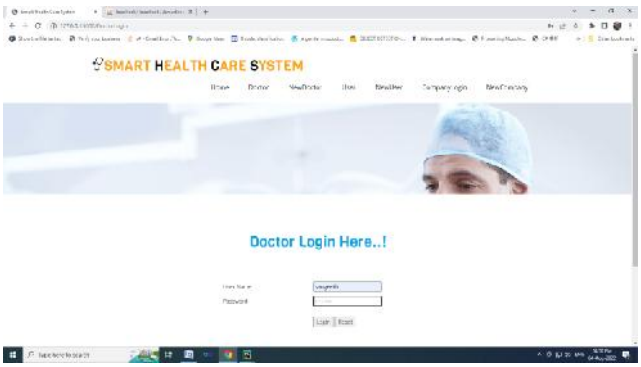
The secure storing of health records via blockchain technology is explained in this module. This framework includes the processes for logging in as a doctor, a user, registering a new user, and an insurance company.



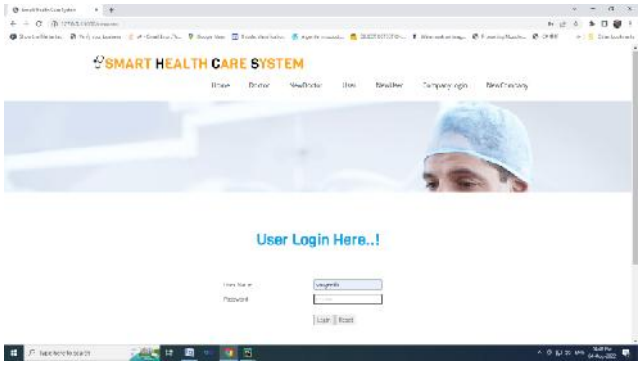
ADMIN CREDENTIALS

About admin credentials are explained in this module. An administrator has access to applications and is responsible for updating applications' specifications. The admin should have the ability to log in, see user information, register new users, and register new doctors, and then assign patients to particular doctors based on their concerns.

Doctor Login



User Login

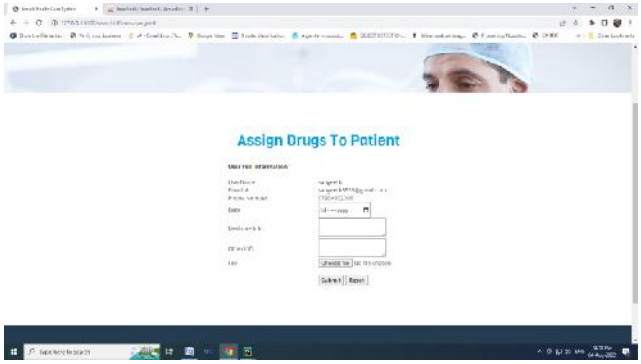


DATA UPLOAD

The procedure of uploading data is explained in this section. The procedures in this framework are as follows: the doctor logs in, views the patient request, confirms the request, and then uploads the patient's reports. Data that has been uploaded is stored using blockchain technology. Data are encrypted with the use of hash code generation.

Doctor Appointment

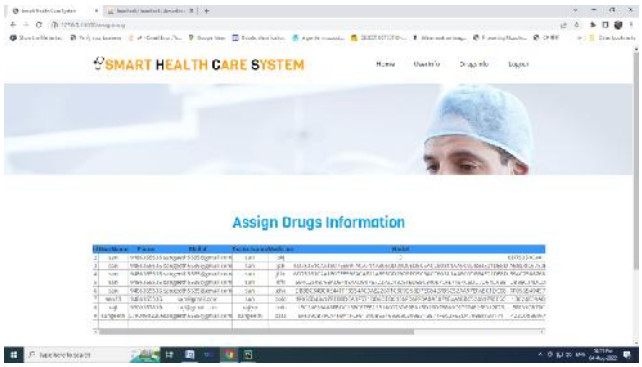
Assign Drugs to Patient



DATA ENCRYPTION

The process of data encryption is explained in this module. The AES technique was used in this case to encrypt the uploaded data. Only authorized users are able to access data using a secret key and decryption technique. Without a secret key, no one else can access the data.

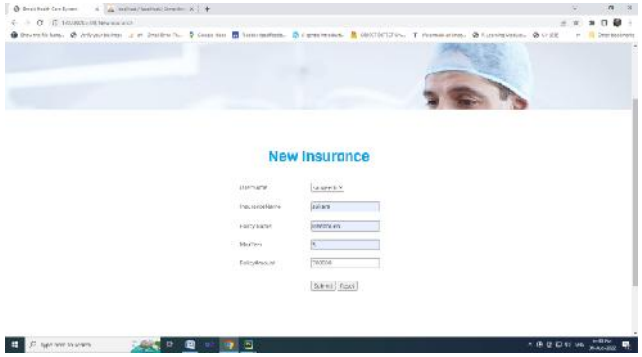
Block chain Technology



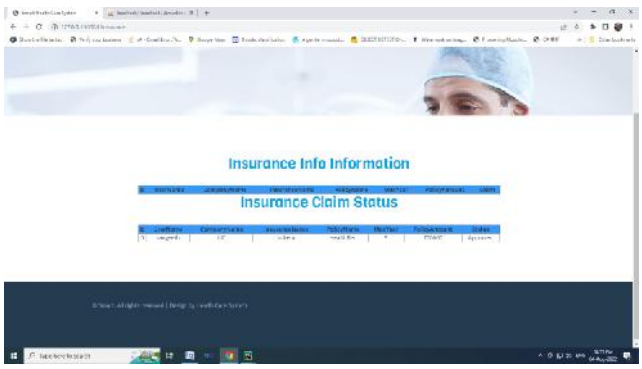
INSURANCE CLAIM

This module provides information on the insurance claim process. The business should sign up and create a login ID. Add policy information to the database after that. Following that, businesses can access user data and send the doctor an insurance request. After receiving doctor permission, the company can submit an insurance claim for the particular patients.

Apply Insurance



Insurance Claim



VI. CONCLUSION

Blockchain technology improves security and usability. The technology has several applications in the healthcare sector, including the storage and sharing of medical data and insurance information in healthcare facilities, remote monitoring systems, and clinical trials.This study proposes an effective access control policy based on user role, as well as secure encryption utilizing the AES encryption technique. To protect data privacy, cloud storage requires secure access management.This suggested blockchain-based storage strategy allows a healthcare company to safely store data in the public cloud. The proposed architecture also efficiently handles insurance claim activities.

REFERENCES

[1] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, ``Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustain. Cities Soc., vol. 39, pp. 283297, May 2018.

[2] W. J. Gordon and C. Catalini, ``Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," Comput. Structural Biotechnol. J., vol. 16, pp. 224230, 2018.

[3] R. Guo, H. Shi, Q. Zhao, and D. Zheng, ``Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 1167611686, 2018.

[4] H. Li, Y. Dai, and X. Lin, ``Efficient e-health data release with consistency guarantee under differential privacy," in Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom), 2016, pp. 602608

[5] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, ``Anonymous authentication scheme for smart cloud based healthcare applications," IEEE Access, vol. 6, pp. 33552_33567, 2018.

[6] U. Premarathneet al., ``Hybrid cryptographic access control for cloud-based EHR systems," IEEE Cloud Comput., vol. 3, no. 4, pp. 58_64, Aug. 2016.

[7] H. Wang and Y. Song, ``Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," J. Med. Syst., vol. 42, no. 8, p. 152, 2018

[8] W. Xu, L.Wu, andY.Yan, ``Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption," J. Comput.Res.Develop., vol. 55, no. 10, pp. 2233_2243, 2018.

[9] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenboloom, ``FHIRChain: Applying blockchain to securely and scalably share clinical data," Comput. Structural Biotechnol.J., vol. 16, pp. 267_278, 2018.

[10] K. Seol, Y.-G.Kim, E. Lee, Y.-D.Seo, and D.-K. Baik, ``Privacy-preserving attribute-based access control model for XML-based electronichealth record system," IEEE Access, vol. 6, pp. 9114_9128, 2018.

[11] Y. Sun, R. Zhang, X.Wang, K. Gao, and L. Liu, ``Adecentralizing attribute-based signature for healthcare blockchain," in Proc. IEEE 27th Int. Conf.Comput. Commun.Netw. (ICCCN), Jul./Aug. 2018, pp. 1_9.

[12] A. A. Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, ``MediBchain: A blockchain based privacy preserving platform for healthcare data," in Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage. Cham, Switzerland: Springer, 2017, pp. 534_543.

[13] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Enforcing role-based access control for secure data storage in the cloud." The Computer Journal 54, no. 10 (2011): 1675-1687.

[14] Gupta, Shubhi, Swati Vashisht, and Divya Singh. "Enhancing Big Data Security Using Elliptic Curve Cryptography." In 2019 International Conference on Automation, Computational and Technology Management (ICACTM), pp. 348-351. IEEE, 2019.

[15] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. "Public integrity auditing for shared dynamic cloud data with group user revocation." IEEE Transactions on Computers 65, no. 8 (2015): 2363-2373.