



(RESEARCH ARTICLE)



Secure healthcare system with insurance processing using blockchain

G Nithya *and Sundar Santhosh kumar

Department of Computer Science, Alagappa University, Tamil Nadu, India.

World Journal of Advanced Engineering Technology and Sciences, 2022, 07(02), 200–211

Publication history: Received on 05 November 2022; revised on 15 December 2022; accepted on 17 December 2022

Article DOI: <https://doi.org/10.30574/wjaets.2022.7.2.0152>

Abstract

Electronic health records provide details about the patient's medications and medical history records. Health information draws attackers' attention since it holds important records. The delivery of the wrong medication or operation is the outcome of the loss of electronic health records. Less security measures are provided by healthcare systems for patient safety information. With the support of particular hospitals, traditional digital health records (EHRs) manage medical information one patient record at a time, which leads to the uncomfortable exchange of records. Cloud-based EHRs are able to share information more easily than traditional EHRs. For cloud-based EHRs, however, a cloud service centre and key generation centre present a specific problem. The proposed effort focuses on developing a new EHR paradigm that can address the centralized issue with cloud-based EHRs. Applying emerging block chain technologies to EHRs is the solution (denoted as block chain-based EHRs for convenience). First, in a block chain scenario, specify the system paradigm of block chain-based EHRs. Additionally, the authentication problem can be crucial for EHRs. On the other hand, the present authentication procedures for block chain-based EHRs have security issues of their own. Additionally, a suggestion for a block chain-based EHR authentication technique is presented here. Our remedy is a collusion-resistant role-based signature system with many signatories that can fend off an attack. Additionally, the suggested method is presumably secure and offers more effective signature and verification processes than current authentication systems in the paradigm of random oracles. The recommended study also focuses on how patients file insurance claims. It helps people get insurance from the authorized insurance sector.

Keywords: Implementation; Blockchain data distribution; Data distribution; EHR sharing

1. Introduction

In a computing context, access control can be used to limit who or what has access to resources. This important security rule reduces the risk to the business or organization. Logical and physical access controls are both available. Physical manipulation is used to impose restrictions on access to campuses, buildings, rooms, and physical IT property. Access to data, files, and computer networks is restricted via logic access control [1].

By analyzing required login credentials, which may include passwords, personal identification numbers (PINs), biometric scans, security tokens, or other authentication components, access control structures identify, authenticate, and provide access to users and entities [2]. In order to protect access to manipulating systems, multifactor authentication, which calls for several authentication factors, is typically utilized as a layer of security.

Access control aims to reduce unauthorized access to both logical and physical resources. Because it guarantees that security technology and access control procedures secure private data, including client information, access control is an essential component of security compliance programming. Recent years have seen a rise in the number of firms installing infrastructure that restricts access to computers, networks, packages, files, and sensitive data, including access

*Corresponding author: G Nithya; Email: nithya13121998@gmail.com

to personally identifiable information and intellectual property. Access control solutions can be difficult to manage in complex IT environments with both on-premises and cloud services [3].

Technology organizations have converted from single sign-on frameworks to unified access management, which integrates access controls for on-premises and cloud settings, in response to some high-profile data breaches.

1.1. Access Control Benefits

Recent years have seen a surge in interest in cloud-based content access, attracting businesses of all sizes and from many sectors. Anyone who has experienced the advantages of cloud-based solutions will not be surprised by that. When compared to conventional, on-premise architecture, cloud-based access controls provide several extremely intriguing qualities, such as streamlined system management and price flexibility. Below are a few noteworthy examples [4].

1.1.1. Accessibility from anywhere with an Internet connection

While some traditional access management programmers 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 enables users to get alerts and take action in the event of a crisis or emergency.

1.1.2. Flexible cost management

Cloud-based services provide significantly more price possibilities, whereas traditional access management programmers typically have high upfront installation and equipment expenditures. 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 staff by contracting with an integrator to host and maintain on-site PCs, servers, data-redundancy infrastructure, and related operations. Depending on the software, a cloud-based solution can minimize the burden of IT participation by 97%. The integrator may be given full or partial control over managing cloud services, depending on the preference of the customer.

1.1.4. System reliability

Keeping all records on a website might be a dangerous task: An energy surge or network failure might impair service functioning or cause data loss if the person doesn't take adequate safeguards. For the security and integrity of the cloud service and data, cloud-based access control solutions typically rely on centralized data centres that are built with reliable backup energy and storage systems.

1.1.5. Round-the-clock updates and monitoring

Software updates and patches are essential for keeping the access management 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 peace 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. Sharing Of Medical Data in the Cloud

Historically, medical information was written down on paper, which was simple to change and harm. The information has to be preserved electronically as a result. The medical database, however, might be altered or even removed. Concern was raised by the information gap as well. Technology is always important when trying to improve quality or

solve issues like resource allocation and information blockage. Data interchange technologies for medical treatment must advance over time. Patients frequently have access to a variety of medical experts, including specialists, general practitioners, and even therapists. Because one illness may have an impact on another, they all need to safely share health records without any modifications. The patient does not need to be an expert or have a sharp memory to recall everything correctly if completely safe data is recorded and transmitted [5].

Patients are required to maintain an accurate medical history file. Furthermore, transferring data through email or even on paper has problems with time, speed, storage, and security. Database data storage has a number of restrictions, such as limited storage space and susceptibility to cyber-attacks. The system could be breached by attackers who would take private patient data.

A centralized database is unreliable due to various access rules for different users, encrypted channel searches, the need for a significant amount of memory to store medical data, and other issues. This strategy has the potential to safeguard data and guarantee reliability. Additionally, as the cloud is a reliable source for data storage and management, cloud computing technology provides for the elimination of storage-related problems. Block chains can also address issues with cloud security. In fact, block chain-powered medical data exchange and cloud storage can address a number of data concerns.

2. Related Work

Guo, et al. [6] Showcase a multiple-authority method for attribute-based identification in which a patient attests to a claim made in reliance on a characteristic without divulging anything other than the evidence that he done so. The patient's public/private keys are also generated and distributed by a number of authorities rather than a single, centralized authority, which solves the escrow issue and corresponds to the storage of dispersed data in a block chain. This approach prevents efforts at cooperation by contaminated authorities by transmitting the secret pseudorandom function seeds among authorities. Furthermore, we clearly demonstrate the security of our attribute-based signature technique in the random oracle model, assuming perfect privacy and computational bilinear Diffie-Hellman signers. Assuming that a cloud storage platform with specific departments, such as hospitals, pharmaceutical firms, and insurance companies, has an EHRs system, sickness research departments, and so on, EHRs systems can be administered jointly. All departments may work together to deliver services to patients while limiting each patient's rights in order to stop the misuse of EHRs.

Dagher, et al. [7] To protect the security of sensitive patient data, it is advised to use a block chain-based architecture allowing patients, providers, and other stakeholders to access medical data in a secure, effective manner. Our suggested system, Ancile, employs six distinct categories of smart contracts in order to operate: consensus, categorization, ownership, permissions, service history, and re-encryption. By using six different contracts, we reduce the amount of effort required managing each contract while allowing patients to benefit from increased utility. By doing this, privacy hazards are reduced while the patient's sense of effectiveness is improved. To achieve a high level of isolation, we leverage the contracts to construct further contracts.

Therefore, it's likely that the patient is the only node who knows directly where their information is located. Ancile employs smart contracts to maintain the cryptographic hashes of the records that are stored and the links between queries in order to guarantee the reliability of EHR databases. Patients can control access to their personal data by utilizing a smart contract to control who has access to it. Patients may also authorize the transplantation of other nodes. This is made possible through identity-checking, which verifies who has access to records, and proxy re-encryption, which avoids the need to re-encrypt the record for each transmission.

Mehmood, et al., [8] Describe a system that protects users of health care applications from attackers and the authentication server by providing them with complete privacy and anonymity. This project's main goal is to offer anonymous authentication so that intelligent cloud-based healthcare systems can guarantee identity privacy. The suggested method can potentially be used for a variety of cloud-based applications and is generally adaptable.

In some circumstances, the actions taken on a particular piece of data over time may be used to identify the user. Therefore, the suggested solution is most appropriate in situations where data processing cannot identify the specific user. Other issues, such query and location privacy in smart health apps, are also crucial. Patients can schedule appointments with doctors or dial an ambulance in an emergency without disclosing their identities.

Wang et al. [9] Make a suggestion for a cloud-based EHR system that uses block chain and attribute-based encryption. In this system, we use IBS for digital signatures and ABE and IBE data encryption to guarantee granular access control

for encrypted data. We offer a unique cryptographic framework known as combined attribute-based/identity-based encryption and signature (C-AB/IB-ES), which combines the attributes of identity-based encryption (IBE) and identity-based signatures with attribute-based encryption (ABE) in multiple ways (IBS).

As a result, the necessity to create numerous cryptographic systems to satisfy various security requirements has been eliminated, considerably simplifying system administration. To further assure that the sources of the data can be identified and that the medical data cannot be changed, we also use block chain technology. As a last phase, a demo application for the medical insurance scene is offered. In this system, patients sign authorization letters granting hospitals access to their data according on their actual needs. The authorization letters are then sent to the block chain data pool to wait for consensus node processing.

Sun and others.[10] suggest that a block chain-based EHR data storage system uses an effective on-chain and off-chain architecture to be able to securely communicate EHR data with numerous CDOs. collaboration storage strategy The advantages of our block chain-based storage solution are as follows: (1) Using block chain to implement secure EHR data sharing between several CDOs such that the data transferred and saved is unmodified, unforgeable, and verifiable(2) To enable large-scale, secure EHR data exchange, use a hybrid on-chain and off-chain storage architecture. Each node off the block chain stores the real EHR data, and each transaction utilizing a block chain includes the address of a single EHR data record. By doing this, the blocks' storage restriction is lifted and users can more easily find each unique EHR data item. The proposed DABS verification protocol's enforceability, security from collusion attacks, anonymity, and non-repudiation should all be carefully examined.

Our experimental research demonstrates the effectiveness and simplicity of the recommended DABS approach.

3. Existing Methodologies

EHRs are used to store all digitally recorded medically pertinent data on the hospital's server. A person might look up prior information such as the patient's and doctor's names, the occasion, the prognosis, and other details prior to visiting a hospital. EHRs are of great interest since the medical business can use them quite effectively. The existing system is trying to create a new EHR framework that will help with problems with cloud-based EHRs. Using cutting-edge techniques Innovation on the blockchain is the solution. In general, a distributed, decentralized database may be compared to a block chain. Traditional application and network architectures, including KGC, cloud service providers, and others, are in charge.

Authentication is a critical component of blockchain-based EHRs. In contrast to block chains, which are anonymous and lack a user authentication method, data in block chain-based EHRs must be authenticated, such as a doctor's diagnosis. As a result, create a reliable authentication solution for block chain-based EHRs. An existing concept for a multi-authority identity-based signature system (MA-IBS) with strong signing and verification algorithms that can thwart collusion attempts.

3.1. Encryption Based on Identity

Revocable-storage identity-based encryption (RS-IBE), which combines user revocation and cypher text updating features, provides the forward/backward security of cypher text.

3.2. IBE

Identity Based Encryption successfully addresses the issue of managing encryption keys (IBE). By employing any string as a public key, IBE can secure data without requiring certificates. Any user can create a public key using identity-based systems using a recognized identifying value, like an ASCII string. Using the Private Key Generator, an authorized third party creates the relevant private keys (PKG). The master public key and associated master private key are first supplied by the PKG. Each user can create a public key that matches the identity ID provided by the master public key by fusing the master public key with the identity value. In response to a request from the user who is permitted to use the identity ID, the PKG generates the personal key for Identity ID using the master key. Without disclosing their key to other participants, users can now encrypt conversations. This is beneficial when technological constraints make pre-distribution of certified keys difficult or impossible. However, the authorized person needs to get the relevant personal key from the PKG in order to decode or sign communications.

3.3. RS-IBE

By using a non-revocable data sharing method, confidentiality and backward secrecy may be guaranteed.

Furthermore, it is possible to provide forward secrecy by using a technique to decrypt and re-encrypt all exchanged data. However, this creates serious issues. It should be emphasized that the entire data sharing system is subject to new attacks because the decryption and re-encryption operations demand access to user private key information. In general, it is not advised to frequently modify the cypher text using a secret key; instead, it should only be used for the best common decryption. Efficiency remains a greater challenge.

The download-decrypt-re-encrypt-upload process must often be finished by the data provider in order to update the shared data's cypher text. This strategy is onerous and unfriendly for cloud clients with limited processing and storage capacity since it results in high connection and compute charges.

4. Sharing Medical Data on Blockchain with Insurance Claim

Researchers proposed basic EHRs as a potential remedy for the issue with information exchange in traditional EHRs. Cloud-based EHRs provide as an excellent illustration of how cloud computing is used in EHRs.

The doctor, pharmacy, diagnostic lab, insurance provider, and other pertinent parties will all provide their medical data to the cloud server. Then, users may utilize the cloud server to search for and download useful data. Data communication between companies that use the same cloud server is simple. Next, when patients switch hospitals, the new hospital may use the cloud to access the patients' medical information, saving them from having to undergo further tests. As a result, the issue of information sharing in conventional EHRs is addressed by cloud-based EHRs. Hospitals and other institutions may only alter medically relevant data when they collaborate with the authority, and EHRs saved in the cloud can only be changed by the authority or the cloud service provider. For data sharing to be practical, only authorized users must have access to the data stored in the cloud.

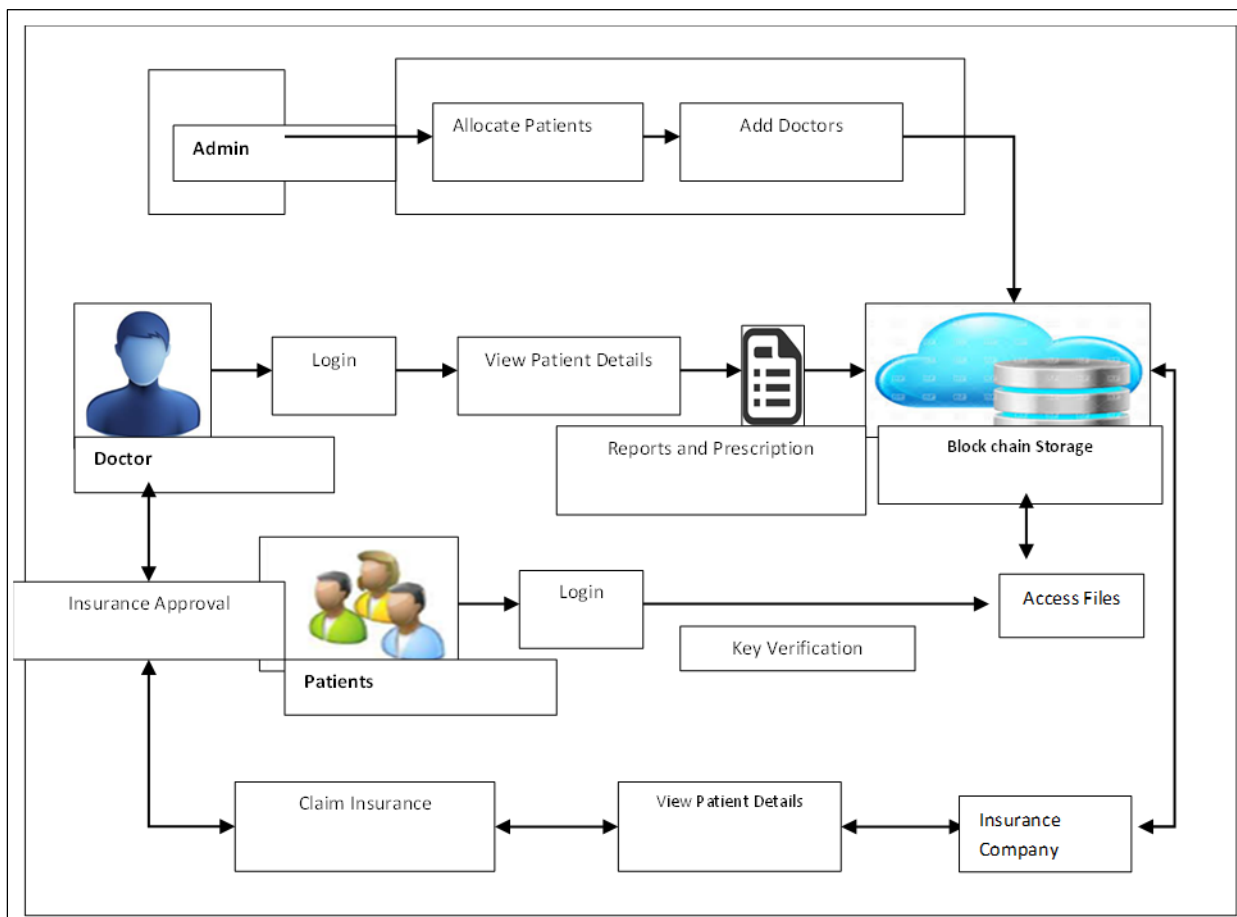


Figure 1 Proposed Work's Architecture

The suggested study makes use of two types of block chain-based EHR users. Level 0, the lowest level, is where the EHRs server is located. Medical insurance providers might be located at level 2, which is represented by Level 1. In block

chain-based EHR systems, all Level 1 users who can agree on the veracity of the data represented by a specific operation would share and store all medically relevant data. Level 2 users produce health-related data, such as medical records from doctors and insurance policies from insurance brokers. The decentralized structure of block chains eliminates this reliance on authorities. This has led to a lot of people thinking about employing block chain in various practical applications, like block chain-based EHRs. The accuracy of such data might be ensured by an appropriate authorization procedure between Level 1 users and their Patients. For stakeholders or authorized users, the suggested structure limits system access. The proposed blockchain-based infrastructure enables the tracking of user activity. Cryptographic techniques are used to authenticate the transfer of patient data. Users and private healthcare data are connected by the technology. To ensure speedy transactions and optimum efficiency, they offered a system that made use of a lightweight block chain. Hospitals and other businesses can only alter medically pertinent data in consultation with the authority, according to the cloud service provider, who also claims that all data in cloud-based EHRs is solely maintained by the authority.

5. Methodology

5.1. Technology Using Block Chain

Data is stored digitally using a concept called a block chain. These structural elements are interconnected, hence their data is unchangeable. A data block's data cannot be changed after it has been connected to the other blocks. Like when it was uploaded to the block chain, it will always be accessible to anybody who wants to see it. The most generally utilized secure algorithms associated with block chain technology are (SHA-1, SHA2, and SHA-256) encryption because of the special quality of hashing operation that yields distinct outputs when given various inputs. In this case, a hash function is a unique key created to separate a transaction from a specific participant in the petroleum supply chain. When used in a hashing crypto method, block chain technology is reliable because it converts bits of fixed-size data into character strings by creating a suitable and reliable hashing algorithm. Each suggested agreement Since the hash data cannot be modified, hash pointers link each block to the one before it. Data is hashed before being put into a block in a block chain.

5.2. Generation of Block and Hash

- A Block that contains information on the most recent transactions.
- A hash is generated for each item of data.
- The components of a hash are letters and integers.
- The database displays the transactions in the order they occurred.
- The most recent transaction's hash as well as that of the most recent transaction both influence the hash.
- No matter how minor, every change to a transaction generates a new hash.
- To make sure a transaction has not been changed, the nodes check the hash.
- If a transaction is accepted by the majority of nodes, it is included in a block.
- The Block chain is made up of discrete blocks that can relate to one another independently.
- A block chain works because copies of it have been made and are available on several computers.

5.3. Encryption using AES

Another name for the AES cypher is block cypher. AES hasn't been the target of any successful attacks. Benefits of using AES include its simplicity on 8-bit computers and its effectiveness when utilized with 32-bit CPUs. Each activity is furthermore open (e.g., XOR, permutation and substitution). The AES encryption process involves several cycles. A round is made up of the four essential operations sub-byte, shift-row, mix-column, and add round key. Bytes from a look-up database are substituted in a process known as sub-byte. Rows are moved one by one using the shift row technique. The mix column times the Galois field matrix.

The output matrix of the mix column has reached the add round key step after being XORed with the round key. The number of encryption rounds required is determined by the key size. These four procedures are employed in a total of nine rounds to generate a 128-bit key, with the last round skipping the mix column step. Since each step is recursive, decryption is the opposite of encryption.

Algorithmic Method the Add round essential step is where the algorithm begins. There are nine rounds in the game, each with four stages, and one final round. Both encryption and decryption follow this rule, with the exception that the decryption technique is completely different at each stage of a round. The four stages are as follows: Modify two bytes.

Change up the columns and rows 3. Here, insert a circular key. In the ninth round, the Mix Columns stage is virtually bypassed.

Following are the first nine rounds of the decryption algorithm:

- Rows that have an inverted shift
- Backward-compatible bytes
- Round Add Key in Reverse
- columns that have an inverse mix
- Again, in the eleventh round, the Inverse Mix Columns stage is merely skipped. Then, we'll examine each of these steps in more detail.

6. Experimental Results and discussion

The experimental findings show how successful the recommended system is. Here, an access control medical data interchange and insurance claim procedure are developed using ASP.NET as the front end and SQL as the back end. This will improve the safety of the files.

6.1. Block Chain Storage

This webinar will discuss the secure storage of medical records using block chain technology. The steps for logging in as a doctor, user, new user, and insurance provider are described in this framework.

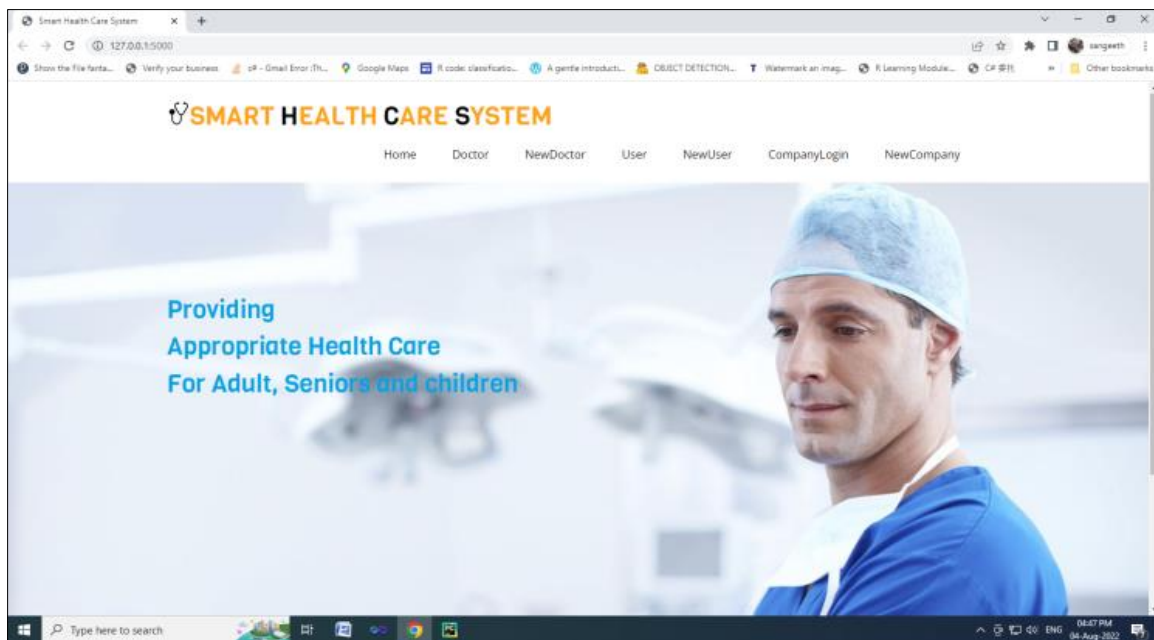


Figure 2 Home Page

6.2. Administrative Credentials

The subject of admin credentials is addressed in this module. Applications can be accessed by an administrator, who is also in charge of upgrading their requirements. The administrator should have access to user information, the ability to add new users and physicians, and the ability to assign patients to certain doctors based on their requirements.

6.3. Doctor Login

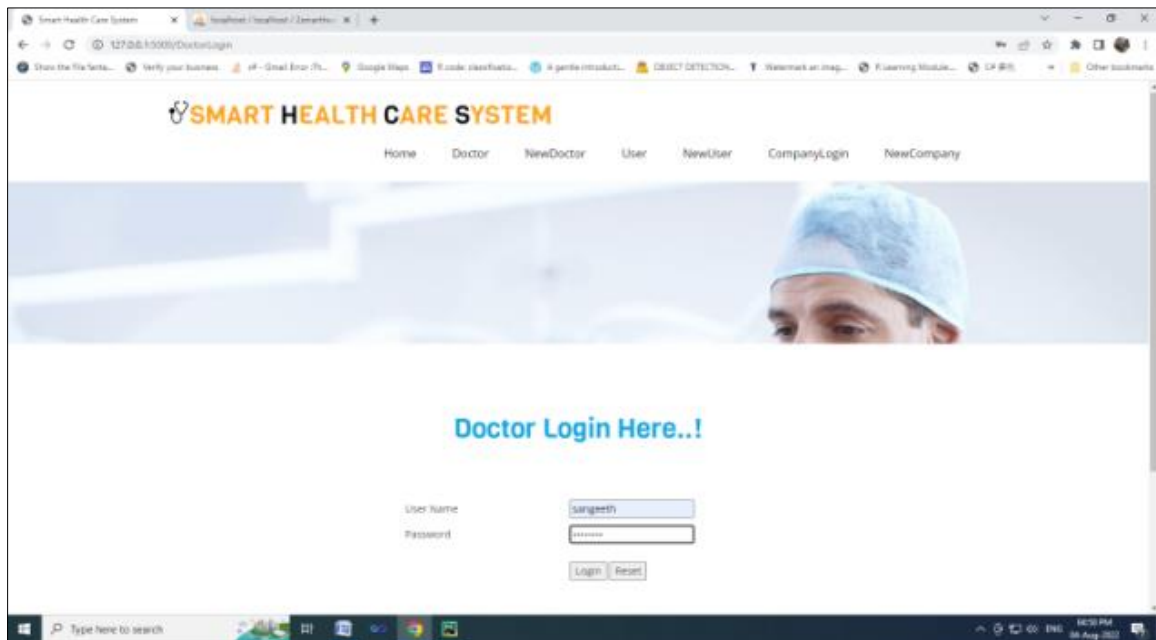


Figure 3 Doctor Login

6.4. User Login

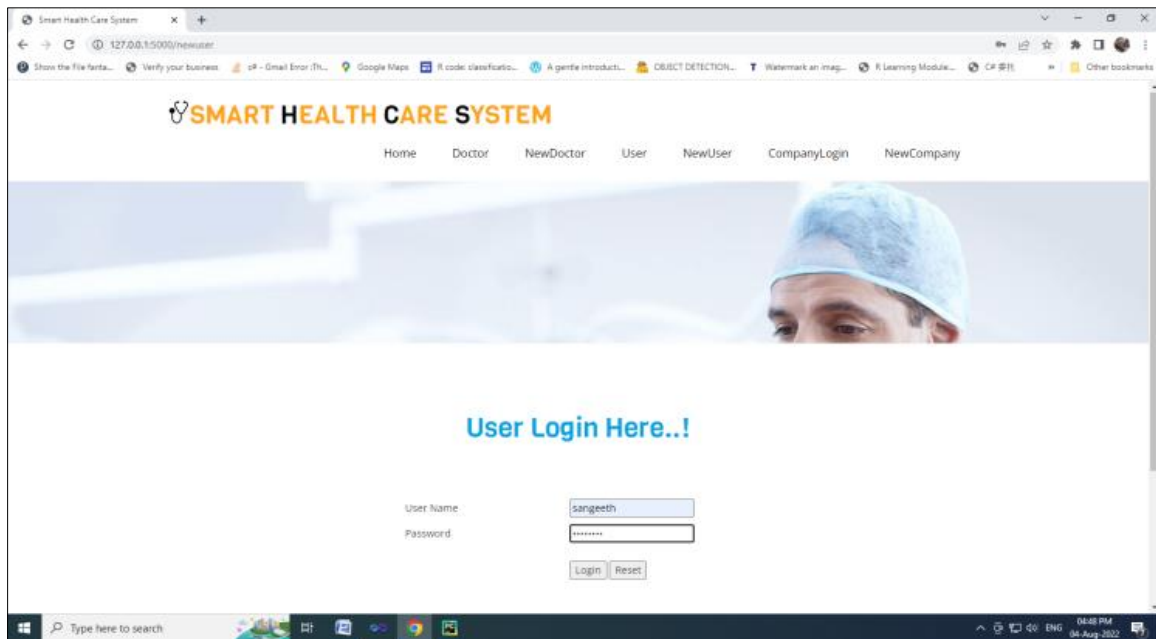


Figure 4 User Login

6.5. Data Upload

In this section, the uploading process is described. According to this structure, the following steps must be taken: the doctor must first log in before viewing the patient request, approving it, and uploading the patient's reports. Block chain technology is used to store provided data. Making hash codes allows for the encryption of data.

6.6. Physician Appointment

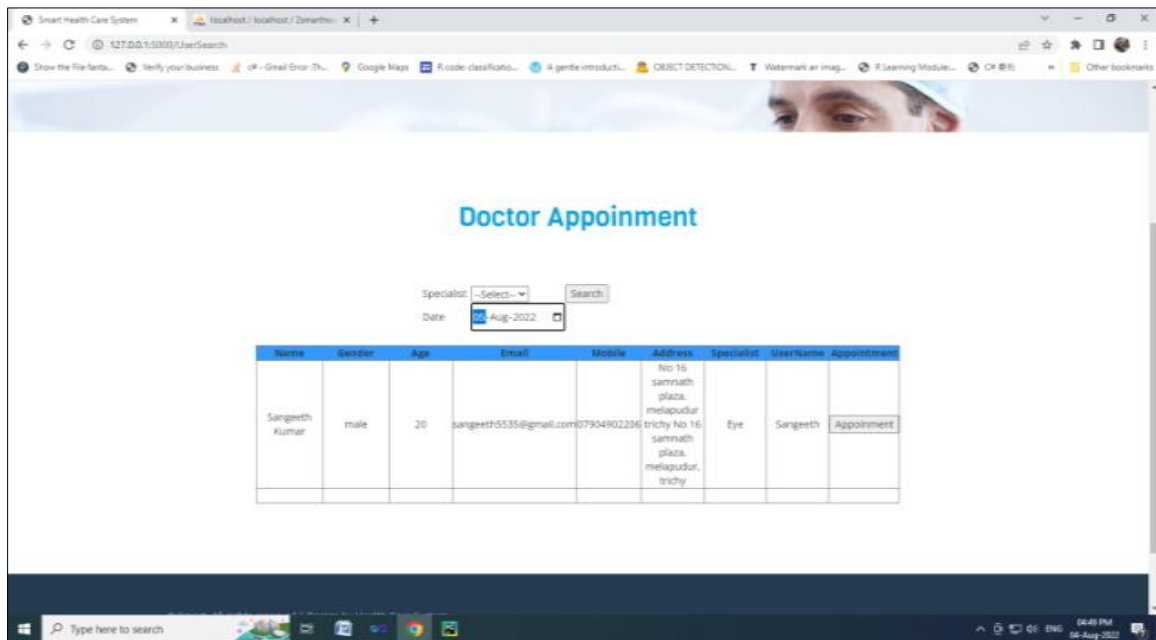


Figure 5 Appointment Page

6.7. Assign Drugs to Patient

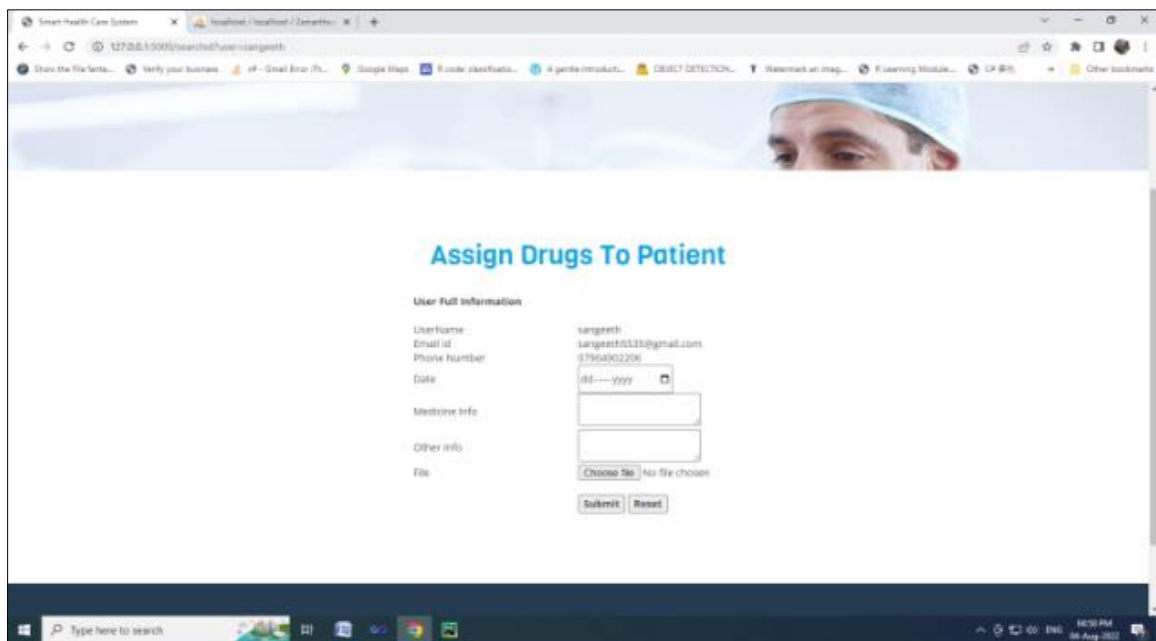


Figure 6 Drugs Assignment

6.8. Data Encryption

This section provides a description of the data encryption procedure. In this instance, the submitted data was encrypted using the AES method. Using a secret key and decryption technique, access to the data is only permitted for authorized users. No one else is able to access the information without the secret key.

6.9. Block chain Technology

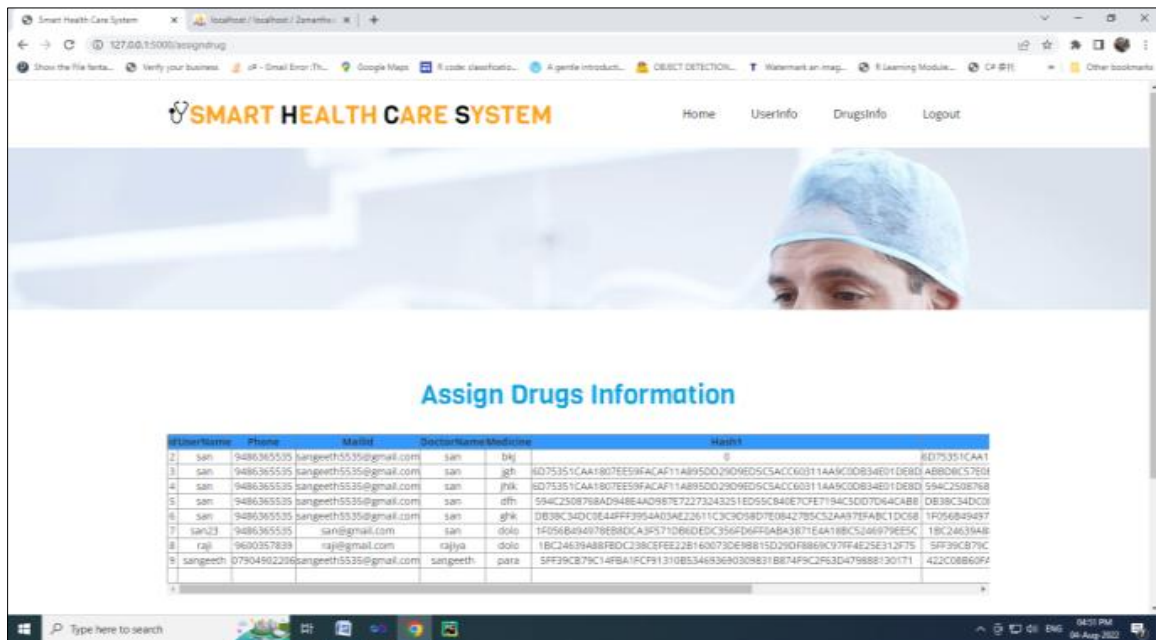


Figure 7 Drug Information Using Block Chain

6.10. Insurance Claim

In this section, the process for submitting an insurance claim is covered. The company must register and create a login ID. After that, add policy information to the database. Then, businesses can access user information and get insurance from the physician. The business may submit an insurance claim for the identified patients after gaining doctor approval.

6.11. Apply Insurance

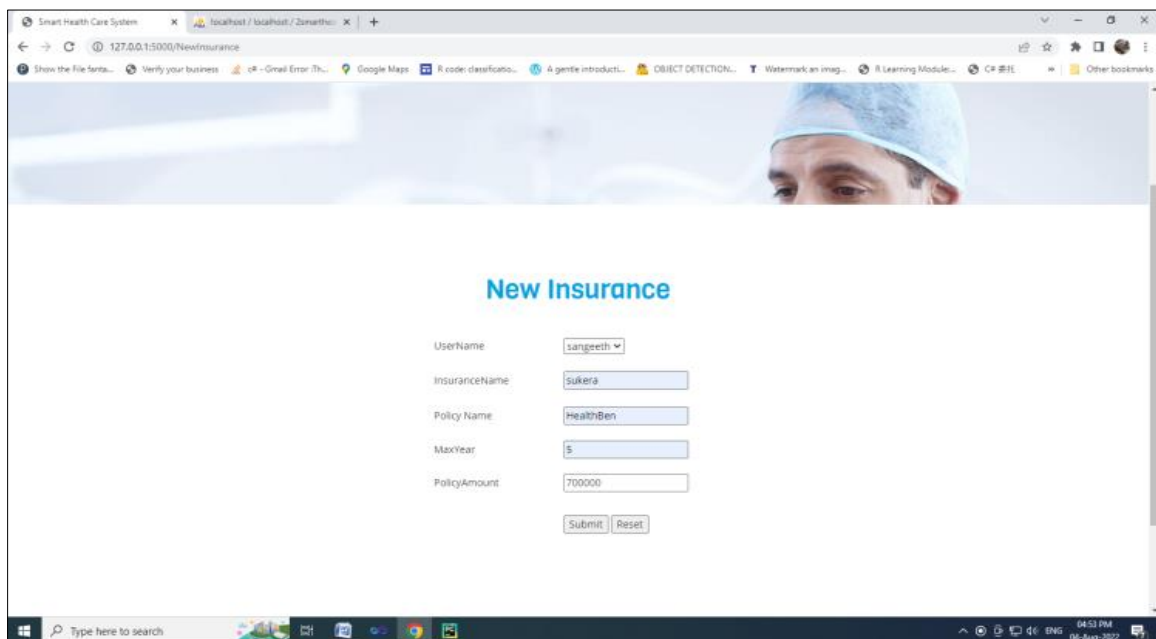
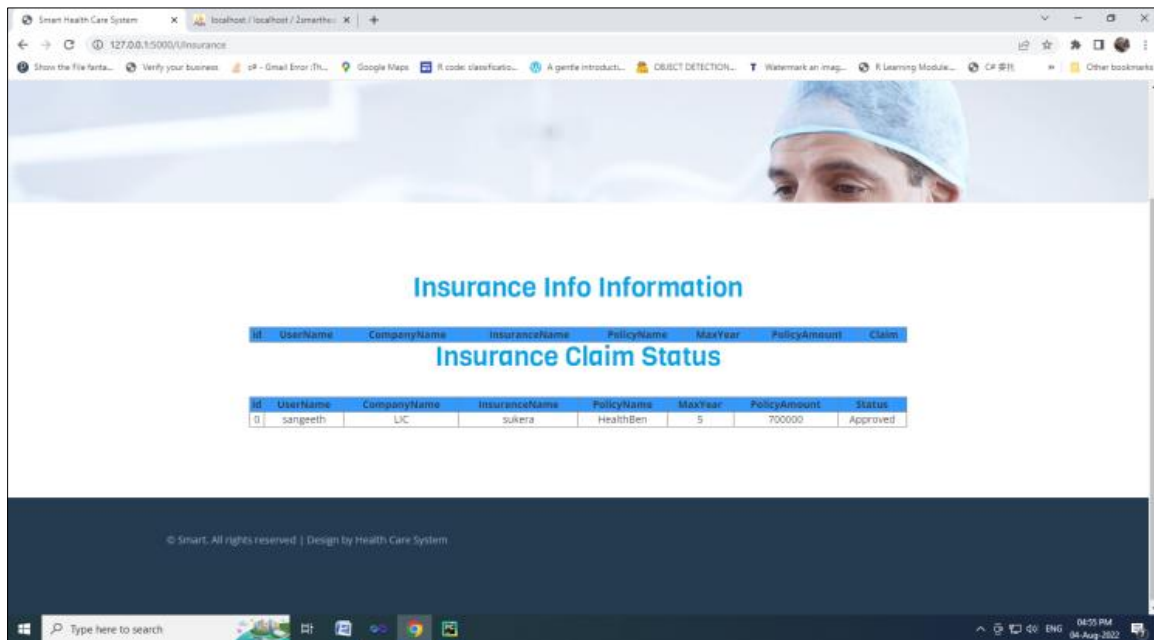


Figure 8 Apply Insurance

6.12. Insurance Claim



The screenshot shows a web browser displaying a page titled 'Insurance Info Information'. Below the title, there are two tables. The first table is titled 'Insurance Claim Status' and contains one row of data. The second table is a header table with columns: Id, Username, CompanyName, InsuranceName, PolicyName, MaxYear, PolicyAmount, and Status.

Id	Username	CompanyName	InsuranceName	PolicyName	MaxYear	PolicyAmount	Claim
0	sangeeth	LIC	sukera	HealthBen	5	700000	Approved

Figure 9 Insurance Status

7. Conclusion

Blockchain technology improves usability and security. A few applications for technology in the healthcare industry include clinical trials, remote monitoring systems, and the storing and sharing of insurance and medical data at healthcare facilities. This research offers strong encryption using the AES encryption technique as well as dependable access control based on user role.

To guarantee data privacy, cloud storage requires safe access management. The suggested block chain-based storage system can be used by a healthcare organization to securely store data on a public cloud. The suggested system also effectively controls insurance claim operations.

Compliance with ethical standards

Acknowledgments

The authors would like to acknowledge Department of Science and Technology, New Delhi for the financial support in general and infrastructure facilities sponsored under PURSE 2nd Phase programme (Order No. SR/ PURSE Phase 2/38 (G) dated: 21.02.2017).

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

- [1] Maselena, Andino, Wahidah Hashim, Eswaran Perumal, M. Ilayaraja, and K. Shankar. "Access control and classifier-based blockchain technology in e-healthcare applications." In *Intelligent Data Security Solutions for e-Health Applications*, pp. 151-167. Academic Press, 2020.
- [2] Brown, Cheryl L. "Health-Care Data Protection and Biometric Authentication Policies: Comparative Culture and Technology Acceptance in China and in the United States." *Review of Policy Research* 29, no. 1 (2012): 141-159.

- [3] Sookhak, Mehdi, Mohammad Reza Jabbarpour, Nader Sohrabi Safa, and F. Richard Yu. "Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues." *Journal of Network and Computer Applications* 178 (2021): 102950.
- [4] Angraal, S., Krumholz, H.M., Schulz, W.L., 2017. Blockchain technology: Applications in health care, *Circulation: Cardiovascular Quality and Outcomes* 10.
- [5] Marwan, Mbarek, Ali Kartit, and Hassan Ouahmane. "A cloud based solution for collaborative and secure sharing of medical data." *International Journal of Enterprise Information Systems (IJEIS)* 14, no. 3 (2018): 128-145.
- [6] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature approach for block chain in electronic health records systems with different authorities," *IEEE Access*, vol. 6, pp. 1167611686, 2018.
- [7] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Confidentiality framework for electronic health record access management and interoperability using block chain technology, *sustain cities society*, vol. 39, pp. 283297, may 2018.
- [8] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Smart cloud-based healthcare apps with anonymous authentication," *IEEE Access*, vol. 6, pp. 33552_33567, 2018.
- [9] H. Wang and Y. Song, "Using a blockchain and attribute-based cryptography, a secure cloud-based EHR system," *J. Med. Syst.*, vol. 42, no. 8, p. 152, 2018.
- [10] Y. Sun, R. Zhang, X.Wang, K. Gao, and L. Liu, "Adcentralizing attribute-based signature for healthcare block chain," in *Proc. IEEE 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul./Aug. 2018, pp. 1_9.
- [11] W. J. Gordon and C. Catalini, "Healthcare block chain technology: easing the move to patient-driven interoperability," *Comput. Structural Biotechnol. J.*, vol. 16, pp. 224230, 2018.
- [12] H. Li, Y. Dai, and X. Lin, "Effective dissemination of e-health data with differentiated privacy guarantee," in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, 2016, pp. 602608
- [13] U. Premarathneet al., "Cloud-based EHR systems with hybrid cryptographic access control," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 58_64, Aug. 2016.
- [14] W. Xu, L.Wu, and Y.Yan, "Electronic health records privacy-preserving plan based on block chain and homomorphism encryption," *J. Comput. Res. Develop.*, vol. 55, no. 10, pp. 2233_2243, 2018.
- [15] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: use block chain to communicate clinical data in a secure and scalable manner," *Comput. Structural Biotechnol. J.*, vol. 16, pp. 267_278, 2018.
- [16] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Access control paradigm with privacy-preserving attributes for XML-based electronic health record systems," *IEEE Access*, vol. 6, pp. 9114_9128, 2018.
- [17] A. A. Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain-based network that protects patient privacy," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, 2017, pp. 534_543.
- [18] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Implementing role-based access control for safe cloud data storage." *The Computer Journal* 54, no. 10 (2011): 1675-1687.
- [19] Gupta, Shubhi, Swati Vashisht, and Divya Singh. "Elliptic Curve Cryptography for Increasing Big Data Security, 2019 International Conference on Automation, Computational and Technology Management. (ICACTM), pp. 348-351. IEEE, 2019.
- [20] Jiang, Tao, Xiaofeng Chen, and Jianfeng Ma. "Public integrity auditing and group user revocation for shared dynamic cloud data." *IEEE Transactions on Computers* 65, no. 8 (2015): 2363-2373.