Health Care Record Data Monitoring in Blockchain Based to Find Malicious Users

G.Lakpathi[1], Medisetty Shivani[2], Vislavath Shirisha[3], Gantekampu Sai Nikhil[4]

[1]*Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana*

[2,3,4]*Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana.*

Abstract

This project aims to enhance the security and functionality of hospital management systems by implementing robust encryption techniques and access control mechanisms. The system allows the addition of doctors, who are required to obtain permission from the hospital before being granted access. Only authorized doctors are permitted to interact with patient data, ensuring that sensitive medical information remains secure. To protect patient data, the system includes an authentication process where user IDs and passwords are verified. If a mismatch occurs, the system detects and flags the access attempt as coming from a malicious user. The system also allows doctors to view patient details and send prescriptions, ensuring a smooth workflow for healthcare providers. Furthermore, medical staff can add and manage medicines within the system. To safeguard sensitive information, the project integrates the use of SHA-256 (Secure Hash Algorithm) algorithm. These data methods ensure that all user data, patient records, and prescriptions are securely encrypted before being transmitted or stored, preventing unauthorized access and ensuring the privacy of all users

Introduction

Busy lifestyles make regular medical checkups difficult for many people, especially for chronic conditions like diabetes and hypertension. Some patients may be less mobile for medical reasons, such as the weak and elderly or those with motion sickness, light sensitivity, or social anxiety. In the recent Covid-19 pandemic, concern about contracting the virus or other illnesses has increased. Remote health monitoring utilizing smart IoT devices could help people unwilling or unable to visit the doctor regularly. Health monitoring IoT devices connect to a mobile app via Bluetooth to share patients' health data with doctors and receive medical suggestions. Such a system, depicted in Figure 1, allows remote medical consultations. Due to the sensitivity of health data and high- security requirements in this domain, a remote health monitoring system must secure user health data at all stages. It is important to ensure (CIA) confidentiality, integrity, and availability of patient data. If patient data is mismanaged or leaked, the lack of privacy will damage the system's reputation, reduce patient trust and hence leave it with few users. All possible threats to patient data must be secured by a successful remote health monitoring system. A large amount of work has been done to secure various aspects of remote monitoring, such as authentication, access control, and secure storage. Notably, Cloud Access Security Broker (CASB) is a complete solution for securing cloud data, monitoring its movement and managing access policies. Several CASB products are available commercially, such as Bitglass CASB, Lookout CASB, CISCO cloudlock and Microsoft Cloud App Security . A CASB provides many security services, including malware detection, cloud configuration, single sign-on for authentication and identity management, user behavior analytics, encryption,key management, and access control. However, even with CASB deployment, insider attacks remain a key challenge. Insider attacks are known to cause significant data breaches. According to the report of *ObserveIT* in 2020, 60% of data breaches were caused by insider attacks. According to a survey by Colombia University researchers, 50% of organizations suffered operational disruption because of insider attacks, 48% reported the loss of critical data

Objective

We will deploy a web application that receives patients' health data (from medical staff, e.g., doctors) and passes it to the CASB to securely store in a public cloud service. Likewise, the web application also receives data retrieval requests and passes them to the CASB to process according to its access control policies, which in turn passes the data back to the web application. Each action of the web application backend and the CASB, whether it is related to data storage or retrieval, is logged immediately into a private blockchain. To be effective at detecting insider attacks, logging systems usually need to be monitored, i.e., someone needs to continuously read the logs and identify when illegal access has occurred.

Literature Survey

S. Sengupta (2022) In this research work, the biometric-based authentication scheme for IoT-based patient monitoring system has been studied. IoT-based patient monitoring system helps the patients to enjoy the healthcare-related services sitting at remote location in their homes. Patient's privacy, safety, and security in this case are very much essential. Authentication technique in this regard is the unique selling point for establishing the safe and secure communication between the patient and the medical server. Jiang et al. have proposed and analyzed a biometric-based authentication scheme in 2017. It was seen that Jiang et al.'s scheme fails to protect the communication system against some of the vulnerable attacks like denial-of-service attack, replay attack, man-in-the-middle attack, offline password guessing attack, smart card stolen attack, forward secrecy attack, user anonymity attack, mutual authentication attack, etc. In order to prevent these security attacks, an enhanced biometric-based authentication scheme using biometric hash function and time stamping in the proposed cryptographic algorithm has been proposed. An informal security analysis of the proposed scheme is also done here. The authentication proof using BAN (Burrows-Abadi- Needham) logic is also done in this paper. For hospitals, a close and prompt monitoring might be required for the critical patients who are admitted in respective critical care units. In order to monitor and diagnose the health of the ailing patients more effectively and efficiently, the smart health application using IoT-based infrastructure with biometric-based authentication system would be required

S. Wang (2022) Electronic medical records can help people prevent diseases, improve cure rates, provide a significant basis for medical institutions and pharmaceutical companies, and provide legal evidence for medical negligence and medical disputes. However, the integrity and security problems of electronic medical data still intractable. In this paper, based on the ciphertext policy attribute-based encryption system and IPFS storage environment, combined with blockchain technology, we constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in IPFS storage environment. Our scheme is based on ciphertext policy attribute encryption, which effectively controls the access of electronic medical data without affecting efficient retrieval. Meanwhile, we store the encrypted electronic medical data in the decentralized Interplanetary File System (IPFS), which not only ensures the security of the storage platform but also solves the problem of the single point of failure. Besides, we leverage the non-tamper able and traceable nature of blockchain technology to achieve secure storage and search for medical data. The security proof shows that our scheme achieves selective security for the choose keyword attacks. Performance analysis and real data set simulation experiments shows that our scheme is efficient and feasible.

M. Ahmed (2023) A computing environment requires a robust and comprehensive process to track and document user activities to uphold confidence in the system. Audit logs are used for this purpose to monitor the actions of administrators and users. However, these logs are vulnerable to multidimensional attacks, including modification of logs, erasability of logs, and privacy of the user. Since administrators have unprecedented access to these logs, they can modify, delete, and even destroy them. Securing these logs against malicious activities is the prime requirement of audit log management. Existing schemes have several limitations, including immutability, computational expensiveness, missing semantics, and are not verifiable. Various schemes have been proposed for this purpose, but a standard method is required to structure heterogeneous logs and their security semantically. To cope with these limitations, in this paper, we propose a Log Management System using blockchain. The proposed system will ensure audit logs' security, which will eventually strengthen users' trust in the computing environment and make it unbreachable even by the administrators. It has been evinced that our model performed better in terms of performance and features already mentioned when compared with existing schemes.

Existing System:

IoT-based remote health monitoring is a promising technology to support patients who are unable to travel to medical facilities. Due to the sensitivity of health data, it is important to secure it against all possible threats. While a great deal of work has been done to secure IoT device-cloud communication and health records on the cloud, insider attacks remain a significant challenge. Malicious insiders may tamper, steal or change patients' health data, which results in a loss of patient trust in these systems. Audit logs in the cloud, which may point to illegal data access, may also be erased or forged by malicious insiders as they tend to have technical knowledge and privileged access to the system

Existing System Disadvantages:

Maintaining privacy regulations
It cannot maintain the malicious data
The attacker we cannot detect

Proposed System

We propose a Cloud Access Security Broker (CASB) model that logs every action performed on user data and secures those logs by placing them in a private by the data owners (i.e., patients). Patients can query the blockchain, track their data's movement, and be alerted if their data has been accessed by an administrator or moved outside the cloud storage. In this work, we practically implement a web application that receives health data from patients, a CASB that securely stores the records in the cloud, and integrate a private blockchain that immediately logs all actions happening in the backend of the web application and CASB. We evaluate the system's security and performance under varying numbers of patients and actions.

Proposed System Advantage

Faster transaction processing and lower costs due to reduced computational requirements.

Organizations maintain control over who can participate and how the network operates

Better suited for scenarios where sensitive data needs to be protected from public view.

System Architecture

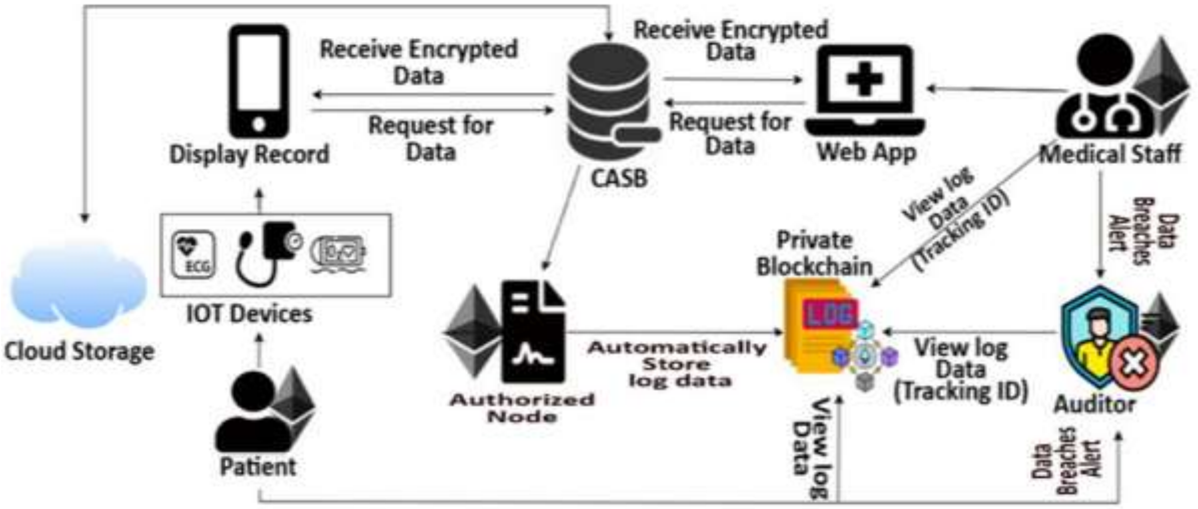


Fig: System Architecture

The proposed A Cloud Access Security Broker (CASB) is a security solution that sits between users and cloud service providers to enforce policies, monitor access, and secure data shared across cloud platforms. In the context of sharing patient data between a patient, doctor, and hospital, CASB technologies can play a key role in ensuring that data is shared securely, privately is designed and focuses entirely on the security of patients. Doctor has a add all information. It was shared a hospital database. Hospital has a register with a all details and logins. Hospital has a all doctor lists the hospital has to approve a doctor. It will get a doctor request. Doctor has takes permission from the hospital. Doctor has a get a patient appointments. Doctor has a view upload reports. Doctor has a live consultations of a patient and doctor they will send messages and discuss a report. Doctor has a patient history. Patient has a register with all details and then login. Patient has a takes a appointment status. Patient has a upload a reports. Patient has also a live consultation. Patient has a history.

Methodologies

1.ONE-WAY HASH FUNCTIONS

A hash function (e.g., SHA-256) is a deterministic mathematical algorithm that receives a message m as input and outputs a fixed-size hash value H(m). For a specific message m, this function always outputs the same hash value.

2.CLOUD ACCESS SECURITY BROKER

A Cloud Access Security Broker (CASB) is a security solution that sits between users and cloud service providers to enforce policies, monitor access, and secure data shared across cloud platforms. In the context of sharing patient data between a patient, doctor, and hospital, CASB technologies can play a key role in ensuring that data is shared securely, privately, and in compliance with relevant regulations (such as HIPAA in the United States). Here's how CASB can facilitate secure data sharing in this scenario:

Modules Name:

1.Hospital

2.Doctor's

3.Patient's

4.Medical Staff

1. User Interface Design

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. Hospital

The Hospital has a register with a id and password. Hospital has add doctors . Hospital has a all doctor list.

3. Doctor's

There are doctor has a register with a details. Doctor has a takes permission from the hospital. Patients also a takes a permission from a doctor. Doctors have a patient appointment. Doctor has a view uploaded a report. Doctor has a live consultations between a doctor and patient. Doctor have a patient history. Doctors has a search by a medicines

4.Patient

There are patient has a register with all details. Patient has a login. Patient has a takes a permission from a doctor.Doctor has a approve. Patient has a appointment status of a doctor. Patient has a upload a diseases reports. Patient has a live consolation of a doctor and patient. Patient has a history of records stores a database.

5. Medical Staff

The has a medical staff login with a user id and password. Emergency doctor has a view a patient lists and Emergency doctor has a view a patient file.

Implementation

A Java implementation for encrypting and sharing medical images securely requires a combination of encryption algorithms, file handling, and possibly networking for sharing. Here's a general plan for building such a solution:

User Interface Design

Input: Enter Login name and Password

Output : If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

Doctors

Input: Doctors has a Login name and Password

Output: If valid user name and password then directly open the Doctors home page otherwise show error message and redirect to the Doctors login page.

Patients

Input: Enter the Patient has a name and password

Output : If valid Patient id and password then directly open the the Patient home page otherwise show error message and redirect to the Patient login page.

Hospital

Input: Enter the Hospital name and password

Output: If valid Hospital id and password then directly open the Hospital home page otherwise show error message and redirect to the Hospital login page.

Medical Staff

Input: Enter the medical staff admin name and password

Output: If valid emergency doctor admin id and password then directly open the medical doctor home page otherwise show error message and redirect to medical login page

Algorithm Used

Existing Algorithm

PRIVATE BLOCKCHAIN

A private blockchain that immediately logs all actions happening in the backend of the web application and CASB. We evaluate the system's security and performance under varying numbers of patients and actions. the web application also receives data retrieval requests and passes them to the CASB to process according to its access control policies, which in turn passes the data back to the web application. Each action of the web application backend and the CASB, whether it is related to data storage or retrieval, is logged immediately into a private blockchain. To be effective at detecting insider attacks, logging systems usually need to be monitored, i.e., someone needs to continuously read the logs and identify when illegal access has occurred. In our case, we would define illegal access as an action performed on user data that is not directly or indirectly initiated by the user. For example, if a doctor updates a patient's record and the patient approves it for upload into the system, the data will be encrypted, indexed, and stored in the cloud.

Proposed Algorithm

1.ONE-WAY HASH FUNCTIONS

A hash function (e.g., SHA-256) is a deterministic mathematical algorithm that receives a message m as input and outputs a fixed-size hash value H(m). For a specific message m, this function always outputs the same hash value.

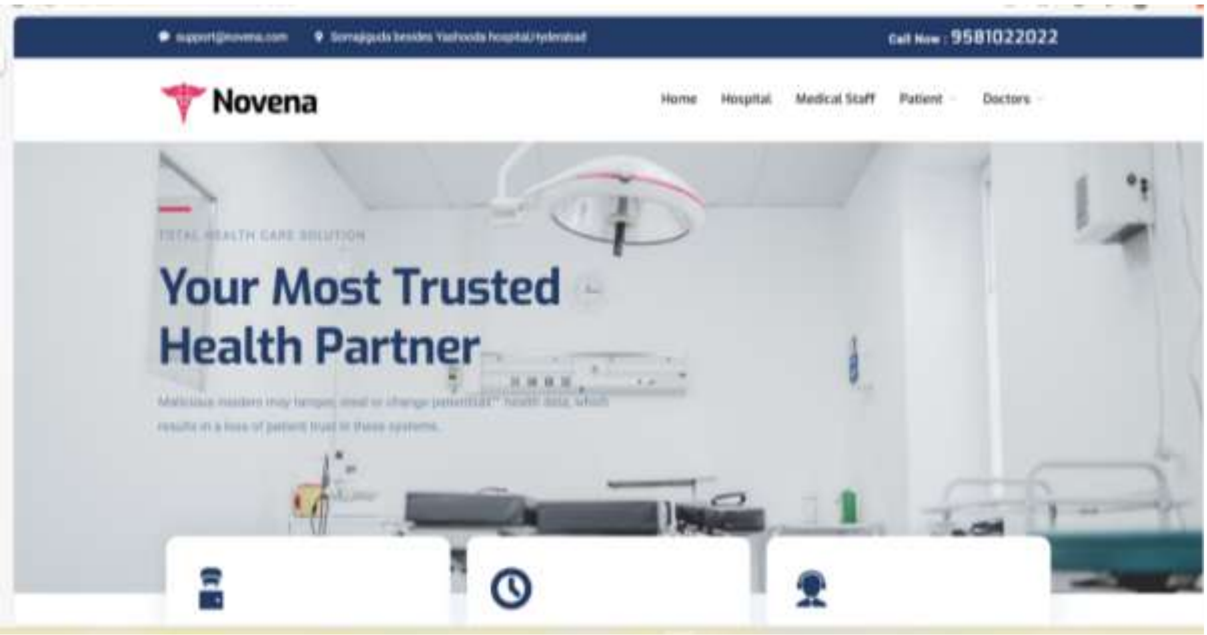
2.CLOUD ACCESS SECURITY BROKER

A Cloud Access Security Broker (CASB) is a security solution that sits between users and cloud service providers to enforce policies, monitor access, and secure data shared across cloud platforms. In the context of sharing patient data between a patient, doctor, and hospital, CASB technologies can play a key role in ensuring that data is shared securely, privately, and in compliance with relevant regulations (such as HIPAA in the United States). Here's how CASB can facilitate secure data sharing in this scenario:

Experimental Results

These pages demonstrate the main features and functionalities of the project, including login, dashboard, hospitals, doctors, medical staff and patient pages.

Interface Page



support@novena.com

Somajiguda besides Yashoda hospital,Hyderabad

Call Now : 9581022022

Novena

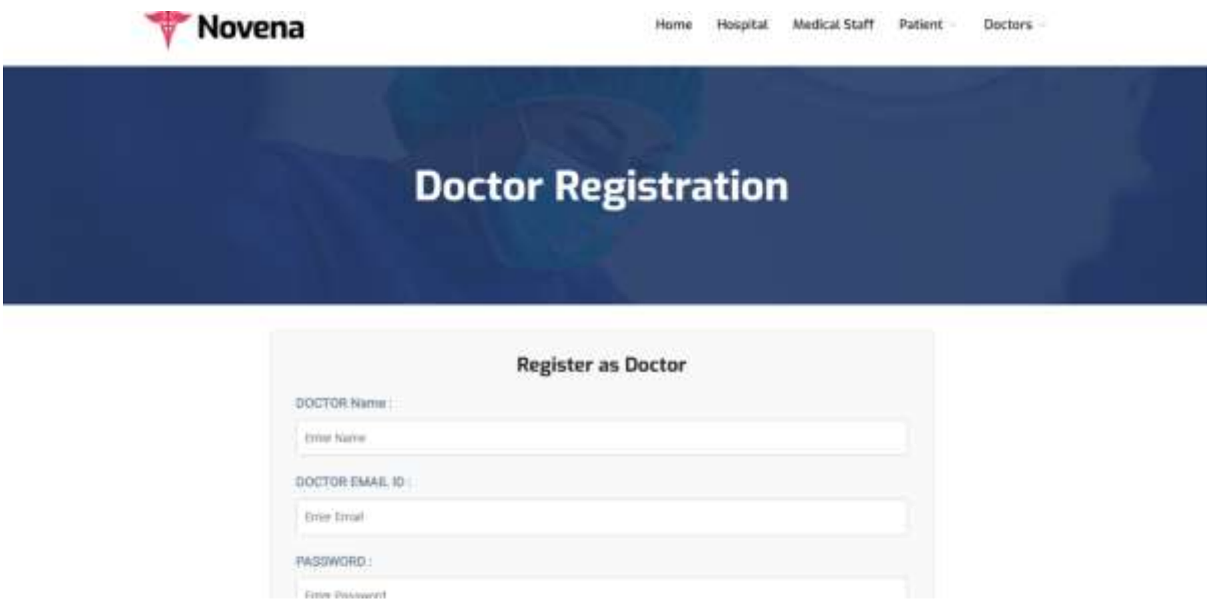
TOTAL HEALTH CARE SOLUTION

Your Most Trusted Health Partner

Malicious insiders may tamper, steal or change patients' health data, which results in a loss of patient trust in these systems.

Interface Page

Registration Pages



Novena

Home Hospital Medical Staff Patient Doctors

Doctor Registration

Register as Doctor

DOCTOR Name :

Enter Name

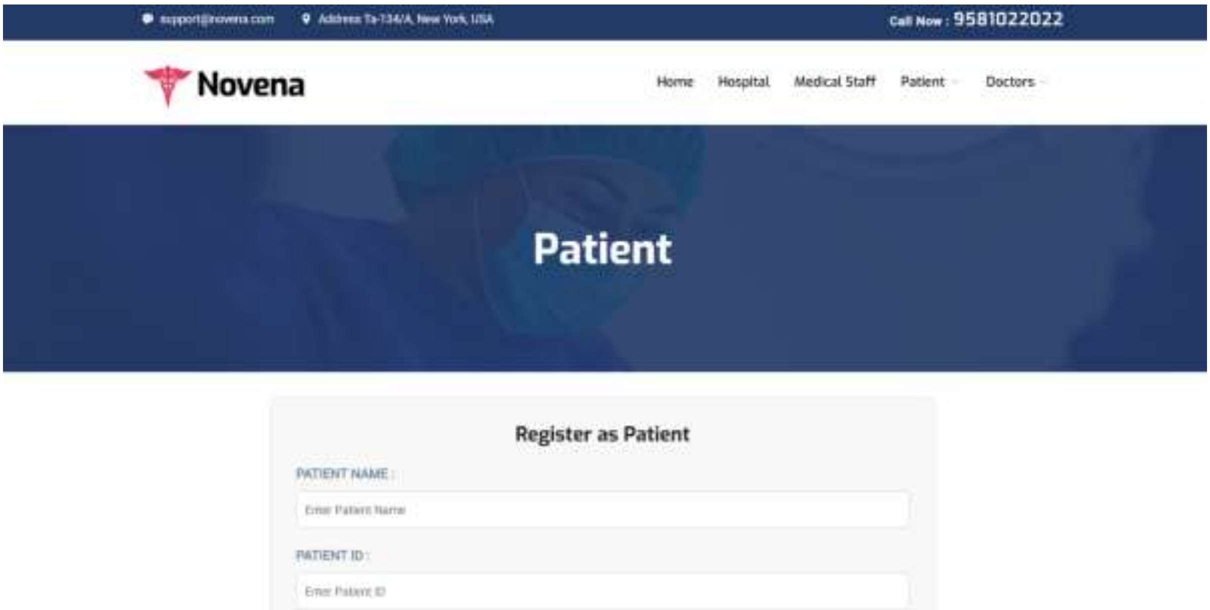
DOCTOR EMAIL ID :

Enter Email

PASSWORD :

Enter Password

Doctor Registration Page



support@novena.com Address Ta-134/A, New York, USA Call Now : 9581022022

Novena

Home Hospital Medical Staff Patient Doctors

Patient

Register as Patient

PATIENT NAME :

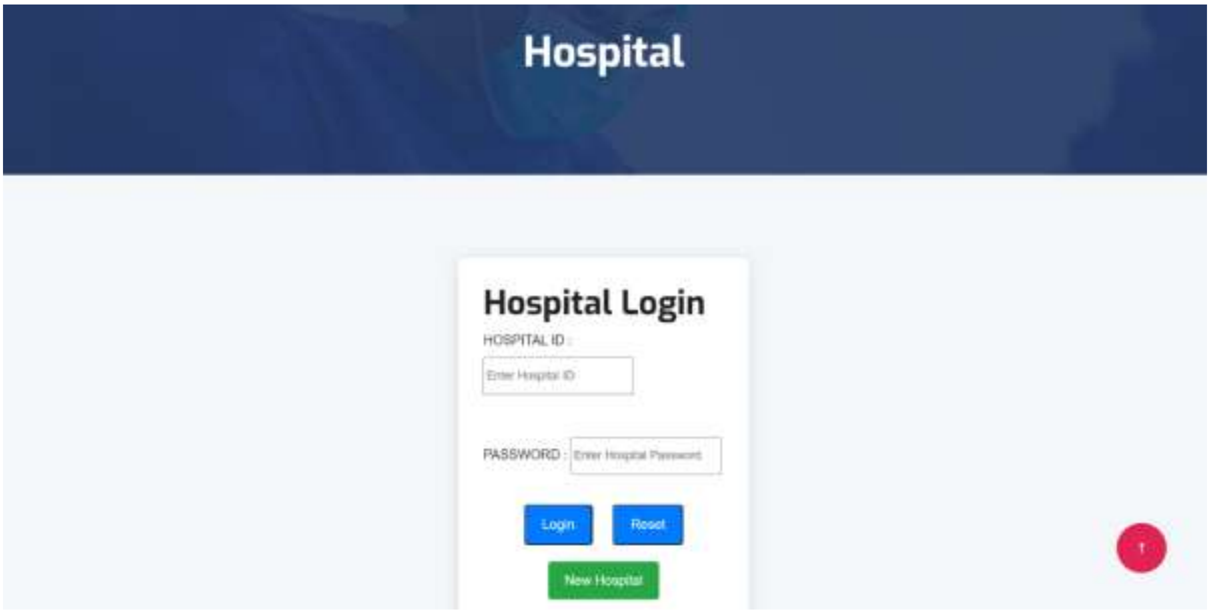
Enter Patient Name

PATIENT ID :

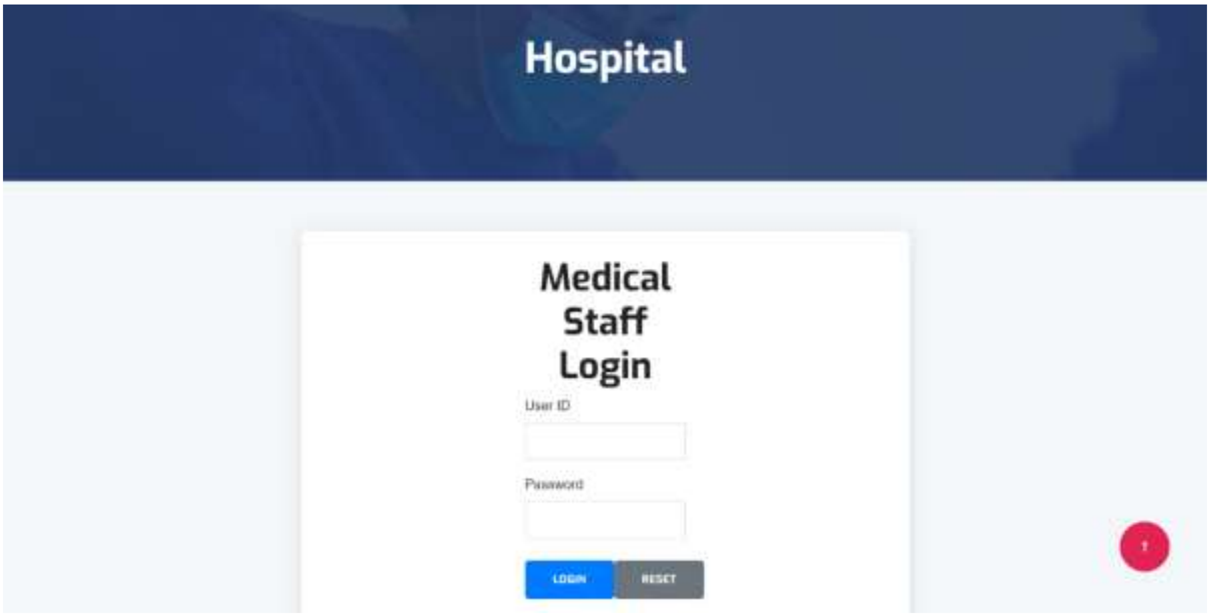
Enter Patient ID

Patient Registration Page

Login Pages



Hospital Login Page



Medical Staff Login Page

Conclusion

We have presented a private blockchain-based remote health monitoring system to protect against insider attacks. The proposed system offers immutability, distribution, and partial decentralization. The two components of our system are the Cloud Access Security Broker (CASB) for managing real health data and a private blockchain to continuously monitor each user's behaviors for detecting insider attacks. CASB would provide end-to-end security, which includes Authentication, Access Control, and Storage, while all user actions are logged and stored in the blockchain. However, due to blockchain's immutability, tampering or theft of log data is not possible. In addition, any user of the system including the auditors, patients, or doctors can search their log data with ID from the blockchain and detect the administrator's malicious behaviors. Moreover, we practically implemented our system using the Ethereum blockchain and evaluated the performance of the system.

Future Enhancement

In the future, the proposed approach will be extended to handle big log data. In the current scenario, we practically implement and test the performance with a small amount of data i.e., KB or MB but with time a large amount of data has been created which may be in GB or TB. Although blockchain has no option to remove data. Moreover, the basic requirement of our proposed system is that nobody can update or delete the log data. Therefore, due to increasing the size of log data in the blockchain, we will require any mechanism to compress this data. but the blockchain also has no option to compress this data. Therefore, the compression process will be possible on the cloud side that compresses every action of the user and stores it in the blockchain also compression does not affect real health data processing. Furthermore, for strong tamper-evidence & audibility, in the future, we may apply ledger DB type stat-of-the art techniques that are capable of facilitating verifiable data removals, a feature that is highly sought after in various practical applications. This functionality allows for the elimination of outdated records to optimize storage space and the concealment of some records to comply with regulatory requirements, all while maintaining the system's capacity to be verified. Similarly, in our proposed system we will integrate private blockchain with CASB (Cloud Access Security Broker) and make like bridge structure but there is a little bit of chance that attackers may be trying to attack this bridge. Therefore, in the future, we will try to apply a hardware-based TPM (Trusted Platform Module) type solution to prevent disabling this logging module entirely.

References

[1]S. Sengupta, "A secured biometric-based authentication scheme in IoTbased patient monitoring system," in Emerging Technology in Modelling and Graphics, 2020, pp. 501–518.

[2]J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," IEEE Access, vol. 8, pp. 59389–59401, 2020.

[3](2022). Bitglass CASB. [Online]. Available: https://www.bitglass. com/casb-cloud-access- security-broker

[4](2022). Lookout CASB. [Online]. Available: https://www.lookout. com/products/casb-cloud- access-security-broker

[5]Cisco Cloudlock. https://www.cisco.com/c/en/us/products/security/ cloudlock/index.html

[6]Microsoft Cloud App Security. https://www.microsoft.com/enus/ security/business/siem-and- xdr/microsoft-defender-cloud-apps

[7]Cloud-Access-Security-Broker-CASB.[Online].Available: https://www. techtarget.com/searchcloudcomputing/definition/cloud-access-securitybroker- CASB

[8]Casb. [Online]. Available: https://www.proofpoint.com/us/threatreference/ casb/

[9]ObserverIT Cost of Insider Threats Global Report 2020. [Online]. Available: https://www.proofpoint.com/us/products/informationprotection/ insider-threat-management

[10]The Colombia University Researchers Perform Survey in 2019. [Online]. Available: https://delinea.com/blog/insider-threats-in-cyber-security

[11]Insider Threats at Hospitals. https://resources.infosecinstitute.com/topic/ insider-threats-at- hospitals/

[12]H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Apr. 2017, pp. 1–3.

[13]T. Yu, Z. Lin, and Q. Tang, "Blockchain: The introduction and its application in financial accounting," J. Corporate Accounting Finance, vol. 29, no. 4, pp. 37–47, Oct. 2018.

[14]P. Gomber, Hinz-O. Nofer M. Schiereck D.,'Blockchain, vol. 59. Cham, Switzerland: Springer, 2017, pp. 183–187.

[15]P. Gomber, Hinz-O. Nofer M. Schiereck D.,'Blockchain, vol. 59. Cham, Switzerland: Springer, 2017, pp. 183–187.

[16]M. Cinque, D. Cotroneo, and A. Pecchia, "Event logs for the analysis of software failures: A rule-based approach," IEEE Trans. Softw. Eng., vol. 39, no. 6, pp. 806–821, Jun. 2013.

[17]S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in Decentralized Business Review, 2008.

[18]F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain- based applications: Current status, classification and open issues," Telematics Informat., vol. 36,

pp. 55–81, Mar. 2019.

[19]T.-V.-L. T.-V. Le and C.-L.-H. T.-V. Le, "A systematic literature review of blockchain technology: Security properties, applications and challenges," J. Internet Technol., vol. 22, no. 4,

pp. 789–801, Jul. 2021.

[20]M. S. Kumar and V. Nagalakshmi, "Secure transfer of robust healthcare data using blockchain-based privacy," Cluster Comput., pp. 1–17, May 2023.

[21]S. Sahai, M. Atre, S. Sharma, R. Gupta, and S. K. Shukla, "Verity: Blockchain based framework to detect insider attacks in DBMS," in Proc. IEEE Int. Conf. Blockchain (Blockchain), Nov. 2020, pp. 26–35.