Blockchain-Based Logging to Defeat Malicious Insiders: The Case of Remote Health Monitoring Systems

Karthik Yeluka (Wells Fargo, Chicago, USA)

Srinivasa Rao Jagarlamudi (Master's in Computers Information Systems, CBU, Memphis, USA)

Eswar Reddy Tippireddy (Bachelor's in Mechanical Engineering, India)

ABSTRACT: Through the use of strong encryption methods and access control systems, this study seeks to improve the security and functionality of hospital management systems. Doctors can be added to the system, but they must first get authorisation from the hospital. Sensitive medical information is kept safe by limiting access to patient data to authorised physicians. The system has an authentication procedure that verifies user IDs and passwords in order to safeguard patient data. The system recognizes and marks the access attempt as originating from a malicious user if there is a mismatch. Additionally, the technology enables physicians to issue prescriptions and see patient information, guaranteeing a seamless workflow for medical professionals. Additionally, the technology allows medical personnel to add and monitor medications. The project incorporates the usage of the SHA-256 (Secure Hash technique) technique to protect sensitive data. By securely encrypting all user data, patient records, and prescriptions prior to transmission or storage, these data approaches guarantee user privacy and prevent unwanted access.

KEYWORDS: BLOCKCHAIN, SHA, HEALTH, DOCTORS, PATIENT.

I.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 [1].

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 [2]. 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 [3], Lookout CASB [4], CISCO cloudlock [5] and Microsoft Cloud App Security [6]. 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 [7], [8]. 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 [9]. 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 and intellectual property, and 37% experienced damage to their brands [10].

These attacks may be perpetrated by a malicious administrator (e.g., disgruntled employees, spies, opportunists looking to expose/sell data for money) who has privileged system access and is familiar with the system policies. As a classical example, a medical device packaging business let go of an employee, Christopher Dobbins, in March 2020. After March, when receiving his last payment, he hacked the company's computer network, gained administrator access, and destroyed 120,000 documents, causing delays in medical equipment delivery [11]. Typical insider attacks in the eHealth domain are tampering, selling, or publishing patients' health data, such as a breach discovered by the Florida hospital where two hospital staff procured patient data sheets, including personal data such as phone numbers, names, and addresses. Two years of data were compromised and possibly used for false insurance claims [12]. The solution to the detection of insider attacks is continuously auditing system activities. For auditing, log data is used to store user actions with timestamps. However, tampering with log data itself is an issue. Malicious administrators with log access can modify log data to cover their tracks after illegally accessing patients' health data. To solve this problem, an immutable logging system is needed. Blockchains present a natural solution for immutability.

II.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.

III.PROPOSED SYSTEM: This paper, we propose a Cloud Access Security Broker (CASB) model that (a) logs every action performed on user data and (b) 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.

There are five modules they are

1. User Interface
2. Hospital
3. Doctor'S
4. Patient'S
5. Medical Staff

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 taken permission from the hospital. Doctor has a get a patient appointment. Doctor has a view upload report. Doctor has a live consultation 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.

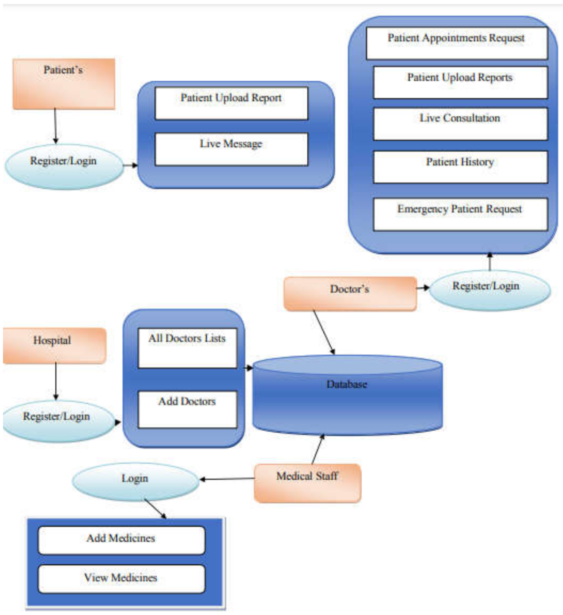
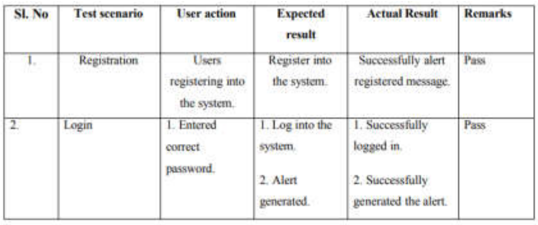
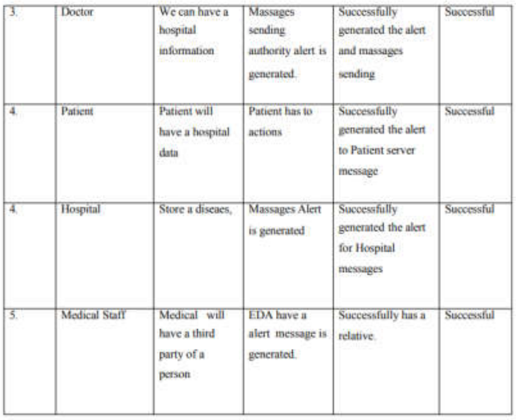


FIG 1 SYSTEM ARCHITECTURE

IV.RESULTS:

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement. The test process is initiated by developing a comprehensive plan to test the general functionality and special features on a variety of platform combinations. Strict quality control procedures are used. The process verifies that the application meets the requirements specified in the system requirements document and is bug free. The following are the considerations used to develop the framework from developing the testing methodologies.

Sl. No	Test scenario	User action	Expected result	Actual Result	Remarks
1.	Registration	Users registering into the system.	Register into the system.	Successfully alert registered message.	Pass
2.	Login	1. Entered correct password.	1. Log into the system. 2. Alert generated.	1. Successfully logged in. 2. Successfully generated the alert.	Pass
3.	Doctor	We can have a hospital information	Massages sending authority alert is generated.	Successfully generated the alert and massages sending	Successful
4.	Patient	Patient will have a hospital data	Patient has to actions	Successfully generated the alert to Patient server message	Successful
4.	Hospital	Store a diseaes,	Massages Alert is generated	Successfully generated the alert for Hospital messages	Successful
5.	Medical Staff	Medical will have a third party of a person	EDA have a alert message is generated.	Successfully has a relative.	Successful

V.CONCLUSION: To defend against insider threats, we have introduced a private blockchain-based remote health monitoring system. The suggested approach provides distribution, immutability, and partial decentralization. Our technology consists of two parts: a private blockchain that continuously monitors user behaviour to identify insider threats and the Cloud Access Security Broker (CASB) that manages actual health data. All user actions are recorded and saved in the blockchain, and CASB would offer end-to-end security, including authentication, access control, and storage. However, log data cannot be altered or stolen because of blockchain's immutability. Additionally, any user of the system, such as auditors, patients, or physicians, can use the blockchain's ID to search their log data and identify any fraudulent actions by the administrator. Additionally, we used the Ethereum blockchain to realistically create our solution and assessed its performance.

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 Cloud lock. https://www.cisco.com/c/en/us/products/security/ cloud lock/index.html

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

7 Cloud-Access-Security-Broker-CASB. [Online]. Available: https://www. Tech target.com/search cloud computing/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 Real world Insider Attack Example. [Online]. Available: https://www.tessian.com/blog/insiderthreats-types-and-real-worldexamples/

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