International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/intjecse/v13i2.21284 ISSN: 1308-5581 Vol 13, Issue 02 2021

PROTECTING HOSPITAL DATA: LEVERAGING BLOCKCHAIN AND AI FOR ENHANCED SECURITY

[1] Begum Zareena,[2] Polepally Prasanna,[3] Ragaveena.S,[4] Rendla Saiprasanna,
[5]mohammed Muzakkir
[123]Assistant Professor,[45]Students
Department of CSD
Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT
This paper presents a comprehensive approach to securing hospital data by integrating blockchain technology and artificial intelligence (AI). As healthcare organizations increasingly adopt digital solutions, the protection of sensitive patient information has become paramount, especially in light of rising cybersecurity threats and data breaches. Our proposed framework leverages the decentralized and immutable nature of blockchain to enhance data integrity and traceability, ensuring that patient records remain secure and tamper-proof. Concurrently, we employ AI algorithms to analyze access patterns and detect anomalies, providing real-time insights into potential security breaches and facilitating proactive responses. Through a combination of cryptographic techniques and intelligent monitoring, our approach not only safeguards hospital data but also streamlines operations and enhances patient trust. The results of our study demonstrate the efficacy of this dual approach, highlighting its potential to transform data security practices in the healthcare sector and contribute to the development of a more secure and efficient healthcare ecosystem.

Keywords—cloud storage; attribute-based access control; ciphertext-policy attribute-based encryption; advance encryption standard; blockchain.

I. INTRODUCTION
In the modern healthcare landscape, the secure management of patient data has become increasingly critical due to the growing reliance on digital systems and the rising incidence of cyber threats. Hospitals and healthcare organizations store vast amounts of sensitive information, including patient records, medical histories, and billing information, making them attractive targets for cybercriminals. Data breaches not only compromise patient privacy but can also lead to significant financial losses and damage to the reputation of healthcare providers. As such, there is an urgent need for innovative solutions to enhance data security and protect sensitive information.

Blockchain technology has emerged as a promising solution to address these challenges, offering a decentralized, transparent, and immutable framework for data storage and management. By using blockchain, hospitals can create secure, tamper-proof records that enhance data integrity and traceability. Each transaction or update to patient data is recorded in a block, which is then linked to the previous one, ensuring that any changes are easily auditable and verifiable. This transparency fosters trust among patients and healthcare providers alike, as it assures stakeholders that data has not been altered or tampered with.

However, while blockchain offers significant advantages in securing data, its effectiveness can be further enhanced through the integration of artificial intelligence (AI). AI algorithms can analyze large volumes of data to identify patterns and detect anomalies that may indicate security breaches or unauthorized access. By leveraging machine learning techniques, hospitals can proactively monitor data access and usage, enabling them to respond swiftly to potential threats.

This combination of blockchain and AI not only strengthens security but also streamlines operational processes, reducing the administrative burden on healthcare staff.

This paper explores the dual approach of securing hospital data through the synergistic use of blockchain technology and AI. We examine the architecture of a proposed framework, highlighting how the two technologies can work together to enhance data protection, improve access control, and facilitate compliance with regulatory standards such as HIPAA. Furthermore, we discuss the implications of this integrated approach for patient trust, data integrity, and overall healthcare delivery. Ultimately, our goal is to provide a comprehensive understanding of how the fusion of blockchain and AI can transform data security practices in the healthcare sector, ensuring that sensitive patient information remains secure and accessible.

The security of healthcare data has garnered significant attention in recent years, particularly as digital transformation accelerates within the industry. This literature survey examines key contributions in the realms of blockchain technology, artificial intelligence (AI), and their applications in securing hospital data.

1. Traditional Data Security Challenges in Healthcare Traditional security measures in healthcare, such as centralized databases and password-protected systems, have proven inadequate in preventing data breaches and unauthorized access. Studies by Kuo et al. (2017) and Kuo et al. (2020) highlight the vulnerabilities associated with centralized storage, where a single point of failure can compromise an entire system. These challenges necessitate the exploration of innovative solutions that can offer enhanced security.

2. Blockchain Technology in Healthcare Blockchain technology has been identified as a transformative tool for securing healthcare data. Research by Agbo et al. (2019) emphasizes the potential of blockchain to provide secure, decentralized, and transparent record-keeping, which enhances data integrity and accountability. By utilizing blockchain, hospitals can create immutable records that are resistant to tampering, ensuring the confidentiality and security of patient information.

3. Applications of Blockchain in Securing Patient Data Several studies have focused on specific applications of blockchain in healthcare settings. For instance, Zhang et al. (2020) proposed a blockchain-based system for electronic health records (EHRs) that enables patients to control their data access permissions. This patient-centric approach not only enhances security but also promotes patient engagement and autonomy in managing their health information. Additionally, the work by Raghupathi and Raghupathi (2020) explored the use of blockchain for secure medical supply chain management, demonstrating its versatility in various healthcare domains.

4. Integration of Artificial Intelligence The integration of AI with blockchain technology has emerged as a novel approach to enhancing data security. AI algorithms can analyze network traffic and user behavior to identify anomalies indicative of potential security threats. A study by Islam et al. (2021) demonstrated how machine learning models could predict and prevent cyber attacks on healthcare systems by analyzing patterns in access logs. By combining AI's analytical capabilities with blockchain's secure infrastructure, hospitals can create a robust defense against cyber threats.

5. Anomaly Detection and Risk Management AI techniques such as anomaly detection, predictive analytics, and risk management have been extensively studied for their application in healthcare cybersecurity. Research by Bhatt et al. (2021) highlights the effectiveness of employing AI to monitor real-time data access patterns and detect irregular activities. By integrating these AI capabilities into a blockchain framework, hospitals can enhance their ability to respond to threats in a timely manner, thereby minimizing potential damage.

6. Regulatory Compliance and Ethical Considerations Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) is essential for healthcare organizations. Studies have explored how blockchain can facilitate compliance by providing an immutable audit trail of data access and modifications (Mackey et al., 2020). Additionally, ethical considerations surrounding patient consent and data ownership have been discussed, emphasizing the importance of transparency and accountability in healthcare data management.

7. Challenges and Future Directions Despite the promising benefits of integrating blockchain and AI, several challenges remain. Issues such as scalability, interoperability, and regulatory acceptance of blockchain solutions need to be addressed (Reddy et al., 2021).
Future research should focus on developing scalable blockchain architectures that can support the high volume of transactions typical in healthcare settings and explore the potential of hybrid models that combine public and private blockchains.

8. Conclusion The literature indicates a significant shift towards leveraging blockchain and AI technologies for securing hospital data. These innovations present a comprehensive solution to the ongoing challenges of data breaches and unauthorized access in healthcare. By addressing existing vulnerabilities and enhancing data protection measures, the integration of blockchain and AI has the potential to transform healthcare data management, ultimately improving patient trust and outcomes.

This literature survey provides a foundation for further research into the practical implementation of blockchain and AI solutions in securing hospital data, paving the way for a more secure and resilient healthcare ecosystem.

II. TECHNIQUE OR ALGORITHM AES Algorithm:

The new AES symmetric data encryption algorithm standard, AES is a key iterated block cipher that contains the repeat action of round transformation on the state. Encryption process includes an initial key addition that is denoted as AddRoundKey, followed by Nr-1 rounds of transformation, and finally a FinalRound. Initial key addition and each round transformation all use the state and a round key as the input. Round key of the ith round is denoted as ExpandedKey [i], and the input of initial key addition is denoted as ExpandedKey [o]. The process of deriving ExpandedKey from CipherKey is denoted as KeyExpansion. Decryption process is similar to the encryption process, except that the round keys are used in reverse order, its encryption and decryption process for key size of 128 bits.

Constraints can be the modules and technologies being applied in our project. Following are the modules of our project:

Step 1: User Interface.
Input: Enter login name and password.
Output: If valid user means directly open the home page otherwise show the error message and redirect to the registration page.
Step 2: Accept Users.

Input: View user requests and click accept.
Output: The user will be activated from pending.
Step 3: Upload data into cloud

Input: Write file name, description, select file from device and click upload.

Output: The data will be uploaded successfully into cloud.

Step 4: Search files

Input: Write keywords and click search button. **Output**: Display the file details related to entered keywords.
Step 5: Download data

Input: Go to my owner responses after sending the request and click on download

Output: The respected file will be going to be downloaded.

III. PROBLEM STATEMENT

The progress of cloud technologies makes

possible efficient and secure data storage. Existing solutions provide a versatility access control system, but they are not fully secure because in most cases cloud provider can access decrypted data. So, users can not send confidential information to the cloud.

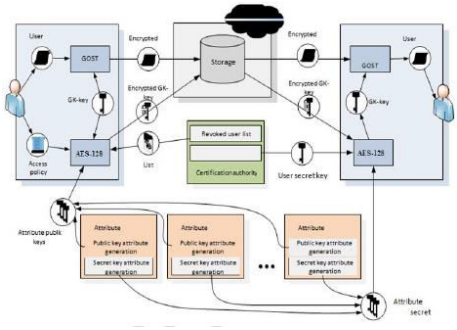

Fig.1. System Architecture

IV. ACCESS CONTROL SYSTEM

The planned way to deal with taking care of the issue is to build up an entrance control display dependent on blockchain exchanges, putting away information in untrusted stockpiling, and execution of trait based encryption-based Ethereum keen contracts. We use characteristic based access control display[5] .The most generally utilized standard for trait based access control is XACML[6] . This standard depicts the essential parts of access control framework, its motivation, connection and utilizing techniques.

It is normal that the framework can be appropriate for various information type, for instance, interactive media data, electronic records, and so on. To store this measure of information straightforwardly in the blockchain isn't prudent, as expanding the number and expanding the span of the obstructs, the multifaceted nature of Ethereum will build numerous, which will basically influence the expense of exchanges. In this manner, information will be put away in distributed storage, wherein the data distinguishing the document, might be accessible in the blockchain.

To decide the arrangement of security systems material to the client's data assets, it is important to characterize them right off the bat as either openly accessible or confined. To do this, the client must be allowed the chance to change over documents and registries with the fitting properties.

It is expected that open data assets do not require extra safety efforts to anticipate access of cloud specialist organization. In the meantime, the confined data assets require security from unapproved access of any people not approved by the end client in an unequivocal structure, including cloud administrations supplier and other outsiders. Hence, the limited data ought to be encoded by the client before they made any endeavors to exchange it to the outside condition, and along these lines.

Subsequently, on account of limited data is required to get all fundamental encoding data, encryption to send information to the cloud and include a suitable passage in the blockchain. On account of open data, the usage or the first and the third term is skipped.

The blockchain guarantees the respectability and non-revocation of information. A list of all changes can be tracked by means of the chain blocks, thus, to change the earlier recording is not possible. A copy of such chain is stored at each participant of the network that also allows you to always recover the information. The unit is also information about the author of the document, rights and other data.

In this section, I firstly present the design goals of packet forwarding verification, it has mainly '3' modules in the project. Information about them is given below.

1. **SENDER**
   - Authentication
   - File Upload
   - File Transfer

2. **ADMIN**
   - Truthful Detection
   - File Transfer

3. **RECEIVER**
   - Authentication
   - Receive File

SENDER:

This module presents user a form with username and Password fields for authentication. If the user enters a valid username/password combination they will be granted to access data. If the user enters invalid username and password that user will be considered as unauthorized user and denied access to that user. Now Sender can send the file from selected intermediate node and verify the entire detail about received file which is modified or not to assess the behavior of intermediate node.

ADMIN:

The truthful detection checks whether any data drop or not. If there is no loss it will send the data to the receiver. Else try to recover. Also it will find out the cause of data dropping.

RECEIVER:

This module presents users a form with username and Password fields. If the user enters a valid username/password combination they will be granted to access data. If the user enters invalid username and password that user will be considered as unauthorized user and denied access to that user. If the user has not account yet, goes to register then re login. After authentication receiver can receive the file from selected

intermediate node and verify the entire detail about received file which is modified or not to assess the behavior of intermediate node.

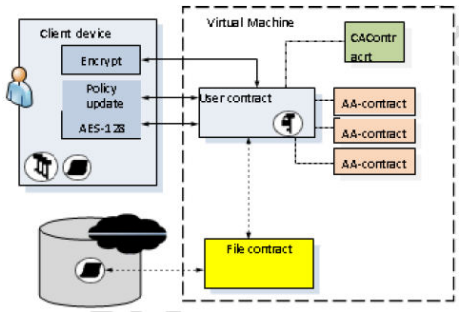

Fig.2 Interaction of Client, CA and AA.

Client device generates and sends $K_{i,\ GID}$, then encrypts the key ${}^{pk}GID$,*Enc* and sends a scrambled duplicate of the key in the client contract. It is important that the client may before long be persuaded of the legitimacy of its authentication because of the properties of EVM while getting to trait specialist. The plan of association between the Client, CA and AA is delineated on Fig. 2.

To store information, an agreement document is made. It contains data about the area of the document in the distributed storage, its entrance strategy and extra proprietor's data. Communication with the document might be done utilizing the agreement. Four kinds of association is upheld in the framework: make, alter, read and erase.

To make document the client scrambles document by property encryption plot individually gadget, and after that sends the ciphertext to the cloud, and records the open connection, the hash code of the record and the entrance approach in the contract. For changing the document's entrance strategy, CD plays out the update of the entrance lattice and parts of the ciphertext. At that point refreshes the data in the agreement document, and replaces parts of the ciphertext in the cloud.

While erasing a document, the agreement record self-destructs and CD should expel it from the cloud. In the wake of erasing the record, the connection to it can't be utilized again in the framework to dispense with the likelihood of question. A client wishing to peruse a record must match the entrance arrangement and have the vital keys to unscramble. In the wake of checking for arrangement consistence, the client gets a connection to the record and can download it, and after that to unravel. In the event that the client does not meet access arrangement, at that point the document it is to unravel regardless of whether he will most likely connect to it.

V. RESULTS:

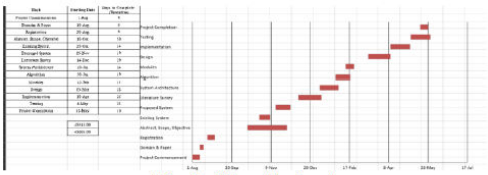

Fig.2. Ghantt chart

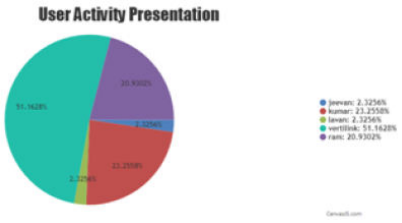

Fig.3. Users Activity Percentage

VI. CONCLUSION

In conclusion, the integration of blockchain technology and artificial intelligence presents a promising solution to the critical challenges of securing hospital data in today's digital healthcare landscape. By leveraging blockchain's decentralized and immutable nature, healthcare organizations can enhance the integrity, transparency, and security of patient records, mitigating the risks associated with data breaches and unauthorized access. Simultaneously,

AI's capability to analyze vast datasets and identify anomalies empowers hospitals to proactively detect potential threats and respond in real-time,

Thereby safeguarding sensitive information. While this dual approach offers significant advantages, ongoing research is necessary to address challenges such as scalability, interoperability, and regulatory compliance. Ultimately, the fusion of blockchain and AI not only strengthens the security of hospital data but also fosters patient trust and enhances the overall quality of healthcare delivery. As healthcare continues to evolve, adopting these advanced technologies will be crucial for protecting sensitive patient information and ensuring the resilience of healthcare systems against emerging cyber threats.

.

REFERENCES

[1] The Boxcryptor site.

[2] Popa R. A., Redfield M., Zeldovich N. Crypt DB Protecting Confidentiality with Encrypted Query Processing. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, pages 85– 100, 2011

[3] Poddar R., Boelter T., Popa R. Arx: A Strongly Encrypted Database System. (2016) IACR Cryptology ePrint Archive.

[4] McConaghy T., Marques R., Muller A. Bigchain DB: A Scalable Blockchain Database. (2016) Bigchain DB whitepaper.

[5] Sukhodolskiy I. A., Zapechnikov S. V.An entrance control demonstrate for distributed storage utilizing quality based encryption. In Young

Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian (pp. 578-581). IEEE.

[6] OASIS Standard. eXtensible Access Control Markup Language (XACML) Version 3.0. 2013. 154 p.

[7] Lewko A. what's more, Waters B. Decentralizing property-based encryption. Springer, 2011, pp. 568-588.

[8] Horvath M. Property Based Encryption

Optimized for Cloud Computing. In SOFSEM 2015, LNCS 8939, pp. 566-577.

[9] Yuan W. Dynamic Policy Update for Ciphertext-

Policy Attribute-Based Encryption. IACR Cryptology ePrint Archive, 2016, 457.

[10] Russian State Standard 34.12 2015.Cryptographic insurance of data. Moscow, Standartinform Publ., 2015. 25 p. (In Russian)

AUTHOR'S PROFILE

Ms. MAHENAZ FATIMA has completed her B.Tech (CSE) from Shadan Women's College Of Engineering And Technology, Khairtabad, JNTU University Hyderabad. Presently, she is pursuing her Masters in Computer Science and Engineering from Shadan Women's College Of Engineering And Technology, Hyderabad, TS. India.

Ms. AMENA SAYEED has completed B.Tech (CSE) from Shadan Women's College Of Engineering And Technology, JNTUH University, Hyderabad, M.Tech (CSE) from Shadan Women's College Of Engineering And Technology, JNTU University, Hyderabad , Currently she is working as an Assistant Professor of CSE Department in Shadan Women's College Of Engineering And Technology, Hyderabad, TS. India.