Blockchain And AI in Healthcare Data Security

[1]Dr.B. Phijik
Assistant Professor, Dept Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd.
email: phijik@gmail.com

[2]Kasivojjula Shivani
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd
email: shivanikasivojjula19@gmail.com

[3] Swetha Nakerakanti
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women, Hyd
Hyd
email: nakerakantiswetha@gmail.com

[4]Chouki Sreeja
UG Student, Dept. Computer Science and Engineering
Vignan's Institute of Management and Technology for Women,

email: srijachouki@gmail.com

Abstract— **Data security and integrity are two essential concepts in the modern era but there are some sectors, which are more sensitive when controlling data. With this project, "Securing Data with Blockchain and AI", it is possible to develop efficient data management by incorporating blockchain and artificial intelligence technology. The healthcare domain in particular is highlighted to demonstrate the practical use of the project focusing on the protection of patient's data. Every transaction creates a hash that is attached to the transaction. Some of the notable features included: hospital and patient logins, patient registration, blockchain hashes displayed during logins, AI search feature for easy access of data. Some of the security implementations include, Secure Hash Algorithm 256 (SHA256), and Advanced Encryption Standard (AES), which will be used to encrypt sensitive data.**

Keywords: Data Security, Data Systems, Artificial Intelligence.

I. INTRODUCTION

Data security has become a critical concern in the modern digital landscape, where vast amounts of sensitive information are generated, transmitted, and stored every second. Emerging technologies like blockchain and artificial intelligence (AI) are playing a transformative role in addressing these security challenges. Blockchain offers a decentralized, tamper-resistant system for recording and verifying transactions. Its use of cryptography and distributed ledgers ensures data integrity, transparency, and protection against unauthorized access or modification. On the other hand, AI enhances security by enabling intelligent systems that can detect threats, analyze anomalies, and respond to cyberattacks in real time. Machine learning algorithms, for example, can continuously learn from data to predict and prevent security breaches. When integrated, blockchain and AI create a powerful framework for

data security—blockchain ensures trust and immutability, while AI adds adaptability and predictive capabilities. Together, they provide robust solutions for secure data management across sectors such as finance, healthcare, and supply chain, paving the way for more resilient and intelligent
digital infrastructures. This powerful integration is being adopted in industries like healthcare, where sensitive patient data must be both secure and accessible; in finance, where fraud detection and secure transactions are essential; and in supply chain management, where transparency and trust are critical. As cyber threats become more complex, the fusion of blockchain and AI is emerging as a future-ready solution for building secure, intelligent, and trustworthy digital ecosystems.

II. LITERATURE REVIEW

The integration of Artificial Intelligence (AI) and blockchain technology has gained significant attention in recent years for enhancing security, privacy, and data integrity across distributed systems. Yin et al. [1] proposed a hyperconnected network as a decentralized paradigm for trusted computing and communication, emphasizing how blockchain can enhance security and transparency in data exchange. Similarly, Fan et al. [2] presented a lightweight RFID protocol focused on securing medical privacy in IoT environments, showcasing blockchain's potential in healthcare data protection. Chaidez et al. [3] explored data isolation from web applications to improve user data privacy, aligning with decentralized frameworks. Lecuyer et al. [4] emphasized the importance of selectivity in big data processing to ensure privacy, a challenge that AI-empowered blockchain systems can address. Montjoye et al. [5] introduced "openPDS," a framework enabling users to manage their own metadata using privacy-preserving technologies. This work is foundational for blockchain systems that promote user sovereignty over data. Perera et al. [6] discussed privacy in open data markets, relevant to blockchain's transparent yet secure data-sharing capabilities. Halvey et al. [7] underscored the power of AI in deriving value from massive datasets, supporting the integration of AI for intelligent blockchain analytics. Lu and Xu [8] applied blockchain to product traceability systems, illustrating practical uses in supply chain transparency. Liang et al. [9] applied deep learning for embedded sensor data analysis in IoT systems, which complements blockchain's secure data storage for such inputs. Xia et al. [10] proposed "MedShare," a blockchain-based medical data-sharing system enhancing secure access across cloud platforms.

III. METHODOLOGY

A. System Architecture

The main goal is to develop a secure, intelligent system that prevents unauthorized access, ensures data integrity, and detects potential threats in real time. Once the objective is defined—such as securing sensitive data transmission or improving intrusion detection—requirements are gathered, including the types of data involved, necessary security features, and user roles. The next step involves designing a hybrid system architecture comprising three main layers: the data layer, AI security layer, and blockchain layer. In the data layer, information is collected from various sources and preprocessed for analysis. The AI layer involves training machine learning models (e.g., decision trees, neural networks, or anomaly detection algorithms) on historical data to identify threats and patterns. These models are then integrated into the system for real-time monitoring and adaptive decision-making.

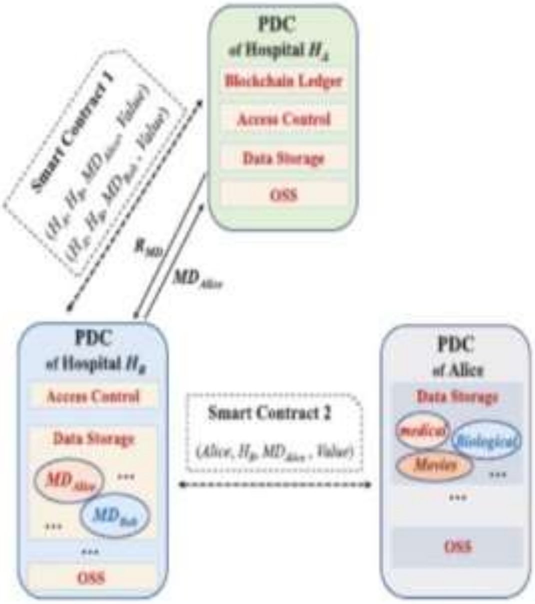

Fig 1: Architecture of data security

Overview

The architecture of the system—termed SecNet—is designed to enhance data security by integrating blockchain and artificial intelligence (AI). It introduces Private Data Centres (PDCs) to manage data securely and independently. Each user has a dedicated PDC that governs their data storage and access, thereby providing full control and transparency.

User Interface Layer: Enables patients and hospitals to interact with the application using simple GUI forms built with HTML/CSS/JavaScript. Application Layer (Django Framework): Handles business logic including data validation, AI-based access verification, and blockchain operations. Blockchain Layer: Ensures data immutability and access control using SHA-256 hashing and transaction records. Database Layer (MySQL): Stores patient data, access permissions, and transaction logs. The architecture supports secure login, patient registration, access permission settings, and smart querying based on disease patterns, powered by basic AI logic

B. Implementation

Blockchain Integration: Each time a patient record is created, a blockchain object is instantiated, and a unique hash is mined to ensure integrity.AI-Based Data Access: When a hospital searches for patient data by disease, the AI logic checks permissions and only reveals records if the hospital is authorized. Reward System: Patients receive reward credits whenever their shared data is accessed by an authorized hospital

IV. RESULTS AND ANALYSIS

RESULT

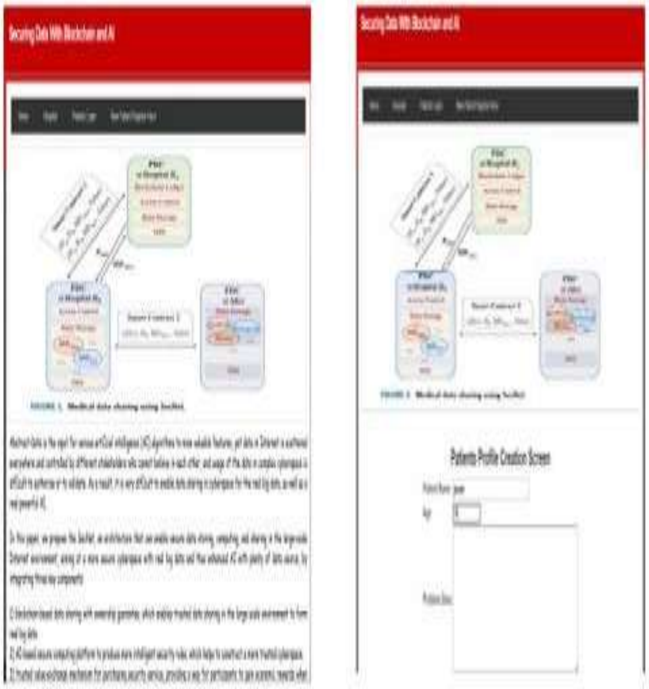
Securing Data With Blockchain and AI
Patients Profile Creation Screen

Fig 2: Medical data sharing using SecNet.

In above screen I am adding patient disease details and selecting ‘Hospital1’ to share my data and if you want to share with two hospitals then hold ‘CTRL’ key and select both hospitals to give permission. Now press ‘Create’ button to create profile.

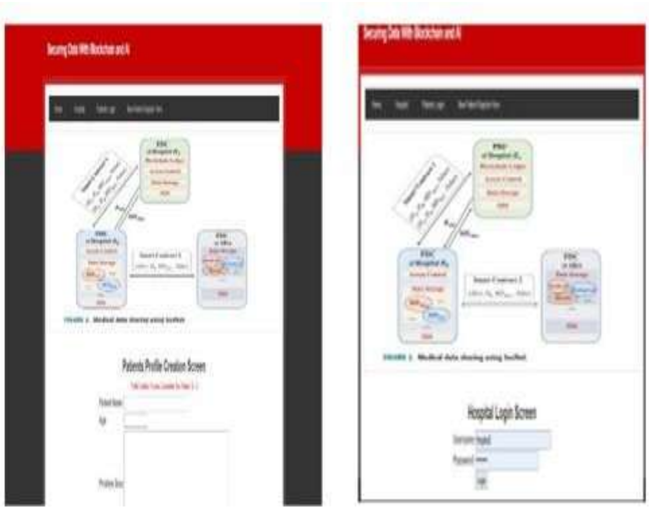
Securing Data With Blockchain and AI
Patients Profile Creation Screen
Hospital Login Screen

Fig 3: Medical data sharing using SecNet.

In above screen one patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1. In above screen to login as Hospital1 click on ‘Hospital’ link to get above screen. Use ‘Hospital1’ as username and ‘Hospital1’ as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen.

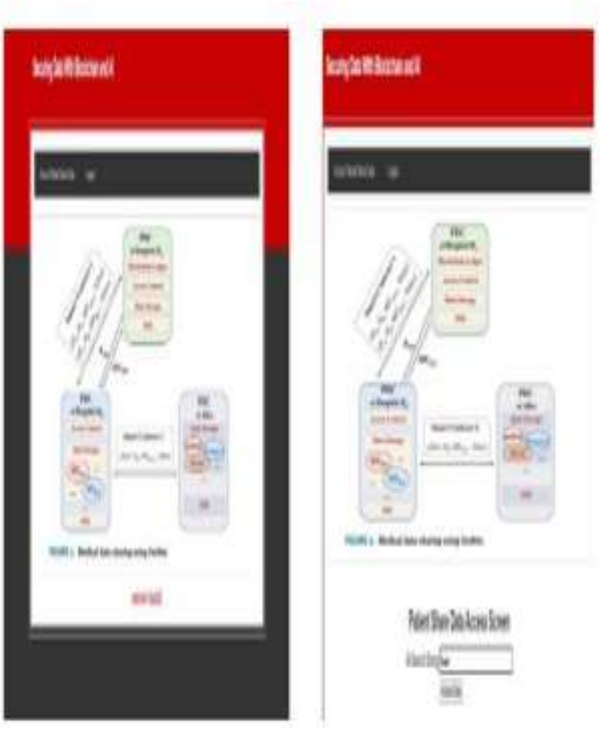
Securing Data With Blockchain and AI
Patient Share Data Access Screen

Fig 4: Medical data sharing using SecNet

In above screen click on ‘Access Patient Share Data’ link to search for patient details. In above screen I want to search for all patients who are suffering from ‘pain’ and then click on ‘Access data’ button to get below screen

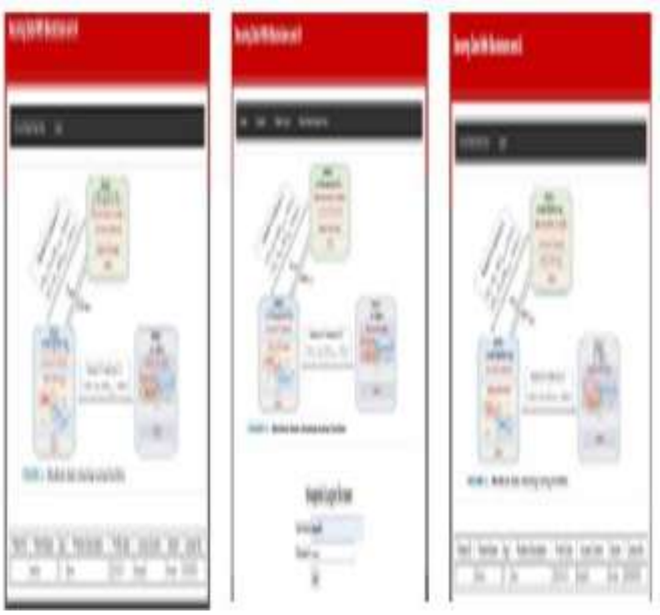

Fig 5: Fig 4: Medical data sharing using SecNet.

In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen. In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'

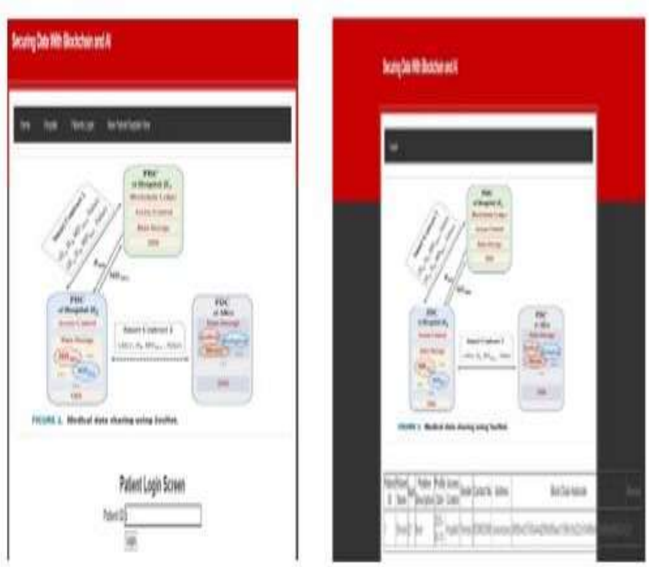
Securing Data With Blockchain and AI
Securing Data With Blockchain and AI
Patient Login Screen
Patient ID

Fig 6: Fig 4: Medical data sharing using SecNet.

In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

V. CONCLUSION

In order to leverage AI and blockchain to _t the problem of abusing data, as well as empower AI with the help of blockchain for trusted data management in trust-less environment, we propose the SecNet, which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating. SecNet provides data ownership guaranteeing with the help of blockchain technologies, and AI-based secure computing platform as well as blockchain-based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to finally achieve better network security. Moreover, we discuss the typical use scenario of SecNet in medical care system, and gives alternative ways for employing the storage function of SecNet. Furthermore, we evaluate its improvement on network vulnerability when countering DDoS attacks, and analyze the inventive aspect on encouraging users to share security rules for a more secure network. In future work, we will explore how to leverage blockchain for the access authorization on data requests, and design secure and detailed smart contracts for data sharing and AI-based computing service in SecNet. In addition, we will model SecNet and analyze its performance through extensive experiments based on advanced platforms (e.g., integrating IPFS [27] and Ethereum [28] to form a SecNet-like architecture). The combination of AI and Blockchain is revolutionizing data security by creating trustless, tamper-proof, and intelligent security mechanisms. Future enhancements will lead to self-learning security systems, real-time fraud detection, and AI-driven decentralized automation, making blockchain networks smarter and more resilient.

VI FUTURE SCOPE

Data security is evolving rapidly with the integration of blockchain and artificial intelligence (AI), offering promising future potential. Blockchain technology enhances data security through decentralization, immutability, and transparency. By distributing data across a network of nodes and using cryptographic techniques, blockchain ensures that once information is recorded, it cannot be altered or tampered with, making it ideal for secure data sharing, audit trails, and identity management. It also provides resilience against cyberattacks like ransomware. However, challenges such as scalability and privacy on public blockchains still need to be addressed with innovations like zero-knowledge proofs and private sidechains.

VII. REFERENCES

[1] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ``Hyperconnected network: A decentralized trusted computing and networking paradigm,' 'IEEE Netw., vol. 32, no. 1, pp. 112_117, Jan./Feb. 2018.

[2] K. Fan, W. Jiang, H. Li, and Y. Yang, ``Lightweight RFID protocol for medical privacy protection in IoT," IEEE Trans Ind. Informat., vol. 14, no. 4, pp. 1656_1665, Apr. 2018.

[3]. T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ``Amber: Decoupling user data from Web applications," in Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV), Warth-Weiningen, Switzerland, 2015, pp. 1_6.

[4] M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen, ``Enhancing selectivity in big data," IEEE Security Privacy, vol. 16, no. 1, pp. 34_42, Jan./Feb. 2018.

[5] Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland, ``openPDS: Protecting the privacy of metadata through SafeAnswers," PLoS ONE, vol. 9, no. 7, 2014, Art. no. e98790.

[6] C. Perera, R. Ranjan, and L. Wang, ``End-to-end privacy for open big data markets," IEEE Cloud Comput., vol. 2, no. 4, pp. 44_53, Apr. 2015.

[7] A. Halevy, P. Norvig, and F. Pereira, ``The unreasonable effectiveness of data," IEEE Intell. Syst., vol. 24, no. 2, pp. 8_12, Mar. 2009.

[8] Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study for product traceability," IEEE Softw., vol. 34, no. 6, pp. 21_27, Nov./Dec. 2017.

[9] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ``Deep learning-based inference of private information using embedded sensors in smart devices" IEEE.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14757_14767, 2017.