International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 2, Mar-Apr 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Blockchain-Infused AI Revolutionizing Health Data Security

Gunnam Srinuvasu, R S S V Prasad, Madugula Sri Krishna Sai Mahalakshmi, Nakka Vijaya Lakshmi, Boggavarapu Venkata Durga Sowmya, Ms.MD.Apsar Jaha
gunnamsrinu123@gmail.com, ravulasurya1@gmail.com, mahalakshmi47474@gmail.com, vijayalakshmin826@gmail.com, boggavarapusowmya07@gmail.com, apsarashu@gmail.com
Pragati Engineering College, Surampalem, Kakinada.Dist, A.P-533437

----------**********----------

Abstract:

In the modern cyber world, data is essential for Artificial Intelligence (AI) algorithms to extract insights from historical data for decision-making, such as product recommendations, healthcare services, or educational institutions. However, not all data, such as sensitive Patient Health Data, can be made publicly available due to privacy concerns. Traditional service providers store user data on third-party servers, often selling it for profit, leaving users with no control. To address this, this project introduces Private Data Centres (PDC) with Blockchain and AI techniques to secure user data. PDC ensures ownership-controlled data sharing via blockchain, intelligent access control with AI-driven verification, and a rewards system to encourage data sharing. This contrasts with traditional Blockchain-based healthcare systems, which use Differential Privacy and Federated Learning t o protect data privacy while focusing on \data utility. The PDC framework promotes data ownership and incentivizes users to participate in data sharing, offering a secure, user-centric approach.

Keywords — **Access Control, Artificial Intelligence, Blockchain, Data Privacy, Django Deployment, Patient Health Data, Private Data Centres, Rewards Mechanism.**

----------**********----------

1. INTRODUCTION

The rapid digitization of healthcare data has significantly advanced artificial intelligence (AI)-driven health analytics, enabling personalized treatment recommendations, predictive diagnostics, and improved healthcare outcomes. However, the sensitive nature of patient health data presents serious challenges regarding data privacy, security, and ownership control. Traditional healthcare data storage models often rely on centralized third-party service providers, which expose data to security breaches and limit patient control over their records [1].

To address these concerns, blockchain technology has emerged as a promising solution for ensuring secure, decentralized, and transparent data management in healthcare. By leveraging cryptographic techniques, blockchain offers immutable record-keeping and access control mechanisms, mitigating unauthorized data modifications and security vulnerabilities [2]. However, merely storing data on a blockchain does not inherently resolve all privacy risks, especially when AI models require access to large-scale datasets for training and inference.

Federated Learning (FL) and Differential Privacy (DP) provide additional layers of security by enabling collaborative AI model training without requiring centralized data storage. FL allows multiple decentralized devices to train AI models locally, ensuring that raw patient data remains private, while DP introduces controlled noise to safeguard individual privacy during AI computations [3]. Despite these advancements, integrating AI, blockchain, and privacy-preserving techniques into a unified framework remains a complex challenge, requiring optimization of model accuracy, security, and efficiency.

This paper proposes a novel Private Data Centre (PDC) framework that integrates blockchain, AI-driven access control, and incentive mechanisms to enhance healthcare data security and usability.

Unlike conventional blockchain-based healthcare models that focus on Differential Privacy and Federated Learning to balance data utility with privacy concerns, the PDC framework introduces ownership-controlled data sharing, AI-powered verification, and a rewards system to encourage responsible data exchange [4]. By leveraging blockchain's decentralization, FL's privacy-preserving model training, and AI's intelligent access control, the proposed framework ensures a user-centric, secure, and scalable approach to managing health data.

The exponential growth of healthcare data, driven by the adoption of digital medical records, wearable health devices, and remote monitoring systems, has facilitated significant advancements in artificial intelligence (AI)-driven health analytics. These advancements enable personalized treatment recommendations, disease prediction, and improved patient care [5]. However, as healthcare organizations increasingly rely on AI to extract insights from medical data, concerns regarding privacy, security, and data ownership become more pronounced [6]. Patient Health Data (PHD) is highly sensitive and, if exposed, can lead to severe consequences, including identity theft, insurance fraud, and unauthorized data exploitation [7].

2. LITERATURE REVIEW

The intersection of blockchain technology, artificial intelligence (AI), and privacy-preserving techniques such as Federated Learning (FL) and Differential Privacy (DP) has led to significant research efforts in healthcare data security. This section reviews key contributions in these domains, identifying current challenges and gaps that this study aims to address.

2.1. Blockchain in Healthcare Data Security

Blockchain technology has been widely adopted to ensure secure, decentralized, and immutable data management in healthcare. Azaria et al. [1] introduced *MedRec*, a blockchain-based electronic health record (EHR) system that enables secure patient data access and management. The study demonstrated how blockchain ensures data integrity and prevents unauthorized access. Similarly, Xia et al. [2] proposed a blockchain-based data-sharing framework for medical records, emphasizing secure, permissioned access among multiple stakeholders**.**

Despite these advancements, blockchain-based healthcare solutions still face challenges in data privacy and computational efficiency. Blockchain alone cannot provide robust privacy guarantees, as stored data can still be vulnerable to inference attacks if proper anonymization techniques are not applied. Additionally, scalability remains an issue, as storing large volumes of medical records on-chain is resource-intensive and costly [3].

2.2. Federated Learning for Healthcare AI

Federated Learning (FL) has emerged as a privacy-preserving machine learning paradigm that enables collaborative AI model training across distributed devices without exposing raw data [4]. FL has been extensively explored in healthcare, where patient data must remain confidential. Xu et al. [5] applied FL to medical image analysis, demonstrating how decentralized learning improves AI model generalization without requiring centralized data aggregation. Similarly, Li et al. [6] developed an FL-based diagnostic model for predicting diseases from decentralized health records, ensuring patient privacy.

However, FL is not immune to privacy attacks. Nasr et al. [7] showed that FL models are susceptible to membership inference attacks, where adversaries attempt to reconstruct private training data. Additionally, FL models require substantial computational and communication resources, making real-time healthcare applications challenging.

2.3. Differential Privacy for Health Data Protection

To further enhance FL's privacy guarantees, Differential Privacy (DP) has been integrated into decentralized learning frameworks. DP introduces

controlled noise to AI models, preventing adversaries from reconstructing individual patient records from model updates [8]. Dwork et al. [9] formalized DP as a mathematical framework for privacy preservation, proving its effectiveness in protecting sensitive data from inference attacks.

Recent studies have explored DP in healthcare applications. Abadi et al. [10] implemented DP in deep learning models for medical diagnosis, demonstrating that adding noise to model updates can protect patient privacy while maintaining high accuracy. However, the application of DP in FL is not straightforward. Excessive noise can degrade AI model performance, reducing predictive accuracy and limiting practical usability in healthcare analytics [11].

3. PROPOSED SYSTEM

This paper proposes a Private Data Centre (PDC) framework that integrates Blockchain, Federated Learning (FL), and Differential Privacy (DP) to enhance the security, privacy, and usability of healthcare data. Unlike conventional healthcare data storage models that rely on centralized third-party servers, the PDC framework ensures ownership-controlled data sharing by leveraging blockchain for secure and decentralized data access management. Patients retain full control over their data through cryptographic smart contracts, granting or revoking access as needed. Federated Learning enables privacy-preserving AI model training across distributed healthcare institutions, ensuring that sensitive health records never leave local storage while still contributing to global AI-driven insights. To further protect patient confidentiality, the system incorporates Differential Privacy, introducing controlled noise to AI model updates, preventing adversarial attacks while maintaining predictive accuracy. Additionally, to address the computational inefficiencies of blockchain storage, the system adopts a hybrid on-chain/off-chain model, utilizing InterPlanetary File System (IPFS) for efficient storage of large healthcare datasets while ensuring security and immutability. The framework also introduces a blockchain-powered rewards mechanism, incentivizing patients and healthcare providers to share anonymized data for research and medical advancements. Through this integrated approach, the proposed system offers a scalable, privacy-preserving, and user-centric solution for secure healthcare data management and AI-driven analytics.

3.1. Blockchain-Based Data Ownership and Access Control

In traditional healthcare systems, patient data is stored on centralized third-party servers, limiting user control and exposing sensitive health records to security risks. The PDC framework ensures patient-owned data management by leveraging blockchain for decentralized access control. Each patient has cryptographic ownership of their medical records, enabling them to grant, restrict, or revoke access using smart contracts. This ensures that healthcare providers, researchers, and AI models can access only authorized data, enhancing transparency and security. Blockchain's immutable ledger records all access transactions, preventing unauthorized modifications or data breaches.

3.2.Architecture:

The architecture depicted in the image represents a decentralized application (DApp) ecosystem integrating blockchain, cryptography, and decentralized storage. The user interacts with the DApp through a web interface, with MetaMask acting as a gateway for authentication and transaction signing. The DApp communicates with the Ethereum blockchain to execute smart contracts and ensure data immutability, while cryptographic techniques safeguard transactions and user data. Instead directly on the blockchain, the system leverages the InterPlanetary File System (IPFS) for decentralized file storage, linking the files securely through cryptographic hashes. This architecture enhances security, transparency, and decentralization, making it ideal for applications in decentralized finance (DeFi), NFTs, and secure data-sharing platforms.

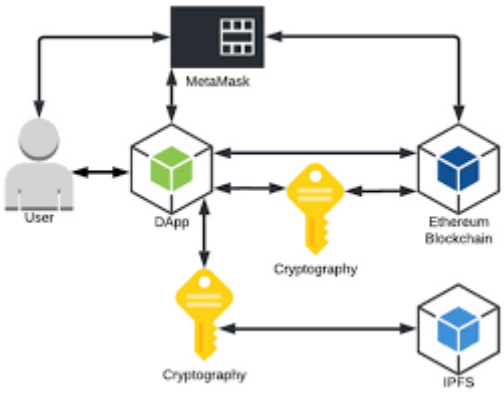

Fig.1.Architecture

3.3.Equations:

\

3.3.1.Blockchain Hashing Function

To ensure data integrity and security, cryptographic hashing (e.g., SHA-256) is used in blockchain to store data securely.

$$H(D) = SHA-256(D) \quad (1)$$

Where:

- H(D) is the hash of the data D,
- SHA-256 is the cryptographic hashing function.

3.3.2. Incentive and Rewards Mechanism

To incentivize users for sharing data securely:

$$R = \alpha . U + \beta . S \quad (2)$$

Where:

- R is the reward,
- U is data utility,
- S is security compliance,
- α, β are tunable coefficients.

4.OUTPUTS AND DISCUSSIONS

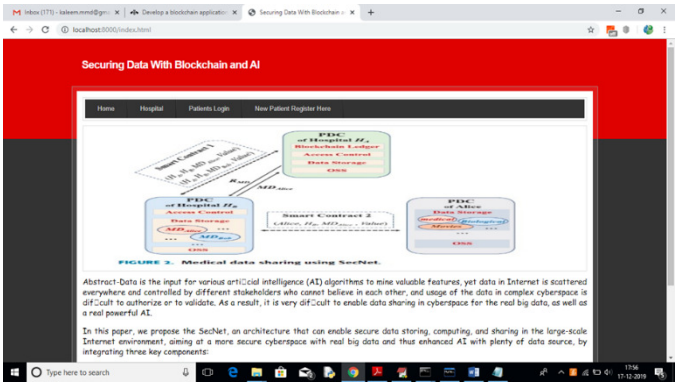

Figure 4.1: Secure Medical Data Sharing via SecNet

Data is the foundation for Artificial Intelligence (AI) systems to derive meaningful insights. However, the decentralized and scattered nature of data on the Internet poses challenges for secure access and trust among different stakeholders. Traditional systems lack the capability to authorize or validate such data effectively in cyberspace, making data sharing and AI training difficult. To overcome this, a secure architecture is essential.This paper introduces SecNet, a novel architecture designed to ensure safe data storage, processing, and sharing in a large-scale Internet ecosystem. It integrates three core components: access control, blockchain-based ledger storage, and smart contracts. The goal is to provide a trusted environment that supports big data sharing and improves AI performance through reliable, real-time, and privacy-preserving data flow.

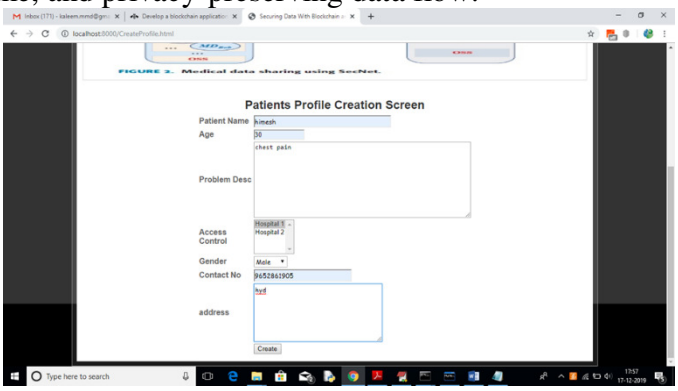

Figure 4.2: Patient Profile Creation Interface

The patient profile creation screen is a front-end interface designed to collect essential patient data in a structured format. It includes fields for the patient's name, age, medical problem description, access control selection, gender, contact number, and address. This information is crucial for

generating unique digital identities for patients and enabling secure data access within the system.

Through this interface, patient data is recorded and integrated into a blockchain-backed system for secure storage and controlled sharing. The access control dropdown ensures that only authorized hospital nodes can access the data, while smart contracts regulate interactions. This design improves data privacy, eliminates duplication, and ensures integrity in medical data handling, supporting secure and seamless healthcare services in the digital environment.

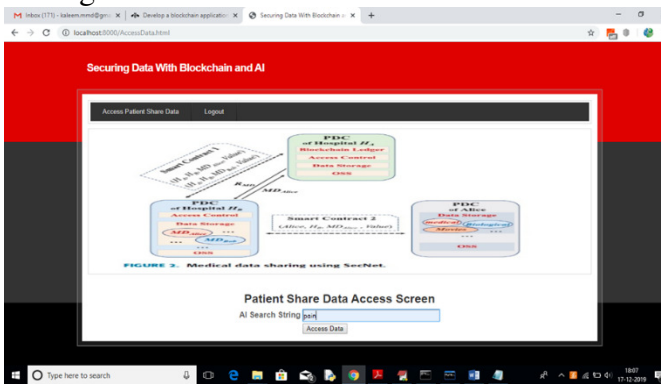

Figure 4.3: Patient Share Data Access Screen – Hospital2

This screen illustrates the AI-assisted patient data access interface for Hospital2, allowing it to retrieve shared patient data based on specific medical keywords or problem descriptions.In this instance, the hospital user is entering the keyword "pain" in the AI Search String field. Upon submission, the system processes this query using AI techniques, cross-references it with shared patient records on the blockchain-secured ledger, and retrieves only the authorized medical data linked to the search string.This feature enhances searchability, precision, and access control in healthcare data management. It also ensures that only relevant and permissioned data is accessed by a hospital based on the smart contract logic, thus maintaining data confidentiality and integrity.

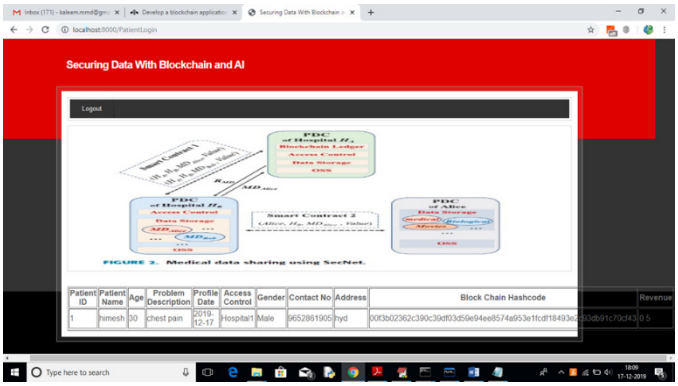

Figure 4.4: Patient Login Screen – Patient Data Access Overview

This figure illustrates the Patient Login Data Access Interface, where patients can securely view their personal and medical information through a blockchain-based platform. Upon successful login, the patient is presented with detailed data including their identification number, name, age, medical condition, the date of profile creation, the associated hospital providing access control, gender, contact number, and residential address. One of the most crucial elements displayed on this screen is the blockchain hashcode. This hashcode serves as a cryptographic signature that ensures the authenticity and immutability of the stored medical record. It guarantees that the data has not been altered or tampered with at any point, thereby enhancing trust and data integrity within the system. The presence of this unique hashcode validates the secure sharing of medical data between hospitals under the SecNet framework. Additionally, any associated financial or revenue-related information is also reflected, providing complete transparency to the patient regarding their medical data transactions. This screen emphasizes the robustness of the system in securing sensitive health data through the integration of blockchain technology.

4.CONCLUSION

The integration of Blockchain and AI in Private Data Centres (PDC) provides a secure, privacy-preserving, and user-centric approach to managing sensitive Patient Health Data. Unlike traditional centralized storage systems that compromise user privacy, PDC ensures ownership-controlled data sharing through blockchain while leveraging AI-driven access control mechanisms. This approach

empowers users by granting them control over their data while fostering trust in healthcare data management. Additionally, the rewards-based mechanism encourages data sharing, facilitating a more collaborative and data-rich environment for AI applications in healthcare. Future research may focus on optimizing the scalability of blockchain in PDC, enhancing AI-driven security measures, and exploring interoperability with existing healthcare frameworks. The proposed PDC model represents a significant step toward revolutionizing health data security by ensuring privacy, accessibility, and user empowerment in the digital era.

FUTURE SCOPE:

The proposed Blockchain-Infused AI framework for securing health data opens several avenues for future research and development. One key area of improvement is the scalability of blockchain networks in Private Data Centres (PDC). Optimizing consensus mechanisms and exploring hybrid blockchain models can enhance transaction efficiency while maintaining security and decentralization.

Another promising direction is the integration of advanced AI models for dynamic access control and anomaly detection. Federated Learning combined with Explainable AI (XAI) can provide enhanced privacy-preserving analytics while offering transparency in decision-making. Furthermore, incorporating homomorphic encryption and zero-knowledge proofs (ZKP) can further strengthen data privacy without compromising usability.

Interoperability with existing healthcare infrastructures and compliance with global data privacy regulations (such as GDPR and HIPAA) are critical areas for future exploration. Standardized frameworks enabling seamless interaction between blockchain-based PDCs and Electronic Health Record (EHR) systems will drive broader adoption.

Additionally, the adoption of token-based incentives for secure data sharing can be further refined through decentralized finance (DeFi) models. These mechanisms can encourage ethical data exchange while preventing exploitation and ensuring fair compensation for users.

Finally, real-world deployment and evaluation of the PDC framework in large-scale healthcare environments will provide empirical insights into performance, security, and user acceptance. Future research should focus on addressing computational overheads, reducing energy consumption, and enhancing the usability of blockchain-infused AI systems for widespread deployment in healthcare ecosystems.

The continuous evolution of AI and blockchain technologies presents a transformative opportunity to revolutionize health data security, ensuring privacy, transparency, and user empowerment in digital healthcare**.**

REFERENCES

[1] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings of the IEEE International Conference on Open and Big Data (OBD)*, Vienna, Austria, Aug. 2016, pp. 25–30.

[2] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information Systems Frontiers*, vol. 22, no. 3, pp. 529–544, Jun. 2020.

[3] M. Kuo, T. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.

[4] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, Jan. 2019.

[5] J. Xu, T. Wang, W. Yang, and H. Li, "Decentralized medical image classification with federated learning," in *Proceedings of the IEEE/CVF Conference on Computer Vision and*

Pattern Recognition (CVPR) Workshops, Long Beach, CA, USA, Jun. 2019, pp. 1–10.
[6] W. Li, S. S. Guo, and X. Liu, "Privacy-preserving federated learning for healthcare systems with edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2086–2095, Mar. 2020.

[7] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *Proceedings of the IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2019, pp. 739–753.

[8] X. Zheng, X. Sun, S. Mukkamala, H. W. Krishnan, and J. B. Wang, "BlockFL: A blockchain-based federated learning framework for secure data sharing in healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 3, pp. 758–768, Mar. 2021.

[9] H. Chen, S. He, D. Wu, and Y. Guo, "Differential privacy-based blockchain for industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4206–4215, Jun. 2020.

[10] Y. Shrestha, R. Sharma, and K. Kant, "AI-driven access control using blockchain for privacy-preserving healthcare data management," in *Proceedings of the IEEE International Conference on Blockchain (ICBC)*, Toronto, Canada, Jul. 2021, pp. 75–82.

