History of Medicine, 2021, 7(2): 236-247

DOI:10.48047.v7.2.2021.14

A BLOCKCHAIN-BASED MODEL FOR STRENGTHENING IOT SECURITY IN MEDICAL DATA

Dr. Persis Urbana Ivy B[1], Akavaram Swapna[1], Nanduri ShankarKumar[1]

[1]Department of Computer Science and Engineering

[1]Sree Dattha Group of Institutions, Sheriguda, Telangana.

ABSTRACT

The Internet of Things (IoT) is in its early stages but is poised to revolutionize daily life by connecting everyday items to the internet. However, as IoT becomes more integrated into our lives, the risk of misuse and cyber-attacks grows significantly. The expansion of IoT into homes and businesses will transform previously offline objects into online systems, widening the surface area for potential cyber-attacks. Current security technologies are insufficient to address these emerging threats.

Blockchain has emerged as a promising solution for enhancing IoT security. This project provides an overview of blockchain technology and its implementation in IoT. We explore how a blockchain-based infrastructure can secure IoT systems, and propose a model to protect IoT devices from vulnerabilities. The goal of this work is to offer practical guidance on using blockchain to create more secure and trustworthy IoT environments.

IoT has numerous applications, including smart homes, smart cities, healthcare improvements, and autonomous vehicles. Several IoT devices, such as wearables, smart thermostats, air conditioners, and refrigerators, are already available, utilizing Wi-Fi for remote monitoring. Despite these benefits, IoT presents serious security challenges. The foundational technologies behind IoT are prone to bugs and vulnerabilities that, if exploited by hackers, could compromise user privacy and cause harm.

As IoT adoption grows, it is crucial to address these issues before large-scale implementation. Strengthening IoT security and eliminating vulnerabilities is one of the biggest challenges facing the industry. In the effort to create affordable, small, and user-friendly IoT devices, many security measures are often compromised, increasing the risk of breaches. This project emphasizes the need for robust security protocols, using blockchain as a key element in ensuring the protection of IoT systems.

Keywords: IoT, cyber-attacks, Blockchain, IoT security, smart devices

1. INTRODUCTION

1.1 History

The integration of blockchain technology with the Internet of Things (IoT) stems from a confluence of developments in both fields. Blockchain, originally conceptualized as the underlying technology for Bitcoin, emerged in 2008 as a decentralized and secure ledger system for recording transactions. Its immutable and transparent nature quickly caught the attention of industries beyond finance, seeking solutions for various challenges, including data security and integrity. Meanwhile, the IoT was gaining traction as an emerging paradigm connecting physical devices and objects to the internet, enabling them to collect and exchange data. However, as IoT devices proliferated, so did concerns about their security vulnerabilities. Traditional security measures were deemed insufficient to protect the vast array of interconnected devices, raising the need for innovative solutions. The synergy between blockchain and IoT became evident as researchers and innovators recognized the potential of blockchain's decentralized architecture to enhance IoT security. By leveraging blockchain's inherent properties such as immutability, transparency, and cryptographic security, IoT systems could be fortified against cyber threats and unauthorized access. Research and experimentation in this area gained momentum in the early 2010s, with academic studies and pilot projects exploring the feasibility and effectiveness of integrating blockchain with IoT. These efforts aimed to address the pressing security challenges posed by the exponential growth of IoT devices and the increasing sophistication of cyber-attacks targeting them. As blockchain technology matured and IoT deployments expanded across various sectors, the integration of blockchain with IoT evolved from a theoretical concept to a practical solution with real-world applications. Today, the fusion of blockchain and IoT represents a promising approach to ensuring the security, integrity, and trustworthiness of IoT ecosystems, spanning smart homes, healthcare, transportation, and beyond.

1.2 Research Motivation

The motivation behind the development of an AI-enabled blockchain system for securing medical data arises from the pressing need to address the security challenges inherent in IoT deployments, particularly in sensitive domains such as healthcare. As IoT devices become increasingly ubiquitous in healthcare settings, collecting and transmitting vast amounts of patient data, ensuring the confidentiality, integrity, and availability of this data becomes paramount. Traditional security measures have proven inadequate in safeguarding IoT devices and the data they generate, leaving them vulnerable to cyber-attacks and breaches. The potential consequences of such breaches in healthcare settings are profound, ranging from compromised patient privacy to disruptions in critical healthcare services. The integration of blockchain technology with IoT presents a compelling solution to these security challenges. By leveraging blockchain's decentralized and immutable ledger system, healthcare organizations can establish a secure and tamper-proof infrastructure for storing and transmitting medical data generated by IoT devices. Additionally, the integration of artificial intelligence (AI) techniques can enhance the security and efficiency of blockchain-enabled IoT systems by enabling predictive analytics, anomaly detection, and automated threat response mechanisms. The research motivation behind this project is to develop a comprehensive framework that leverages the synergies between AI, blockchain, and IoT to create a robust and secure system for managing medical data. By harnessing the power of AI-enabled blockchain technology, healthcare organizations can mitigate the risks associated with IoT deployments, ensuring the confidentiality, integrity, and availability of sensitive medical information.

1.3 Problem Statement

The problem addressed by the AI-enabled blockchain system for securing medical data lies in the inherent security vulnerabilities of IoT devices and the healthcare systems they are integrated with. As IoT devices proliferate in healthcare settings, collecting and transmitting vast amounts of patient data, they become lucrative targets for cyber-attacks and breaches. Traditional security measures are often insufficient to protect against these threats, leaving patient data vulnerable to unauthorized access, tampering, and exploitation. Furthermore, the interconnected nature of IoT devices and healthcare systems amplifies the potential impact of security breaches, posing significant risks to patient privacy, safety, and the integrity of healthcare services. The challenge lies in developing a robust and scalable security framework that can effectively mitigate these risks while ensuring seamless interoperability and usability of IoT devices in healthcare settings.

The AI-enabled blockchain system aims to address these challenges by leveraging AI techniques for predictive analytics and anomaly detection, coupled with blockchain's decentralized and immutable ledger system for securing medical data. However, implementing such a system requires overcoming various technical, regulatory, and organizational challenges, including interoperability issues, data privacy concerns, and regulatory compliance requirements.

2. LITERATURE SURVEY

Rajawat et al.[1] proposed AI and Blockchain based framework for improving the data security in the smart cities domain.Alabdulatifet al.[2] had proposed a architecture which was evaluated using various performance metrics such as blockchain scalability, accuracy, and dynamic malware analysis. Lastly, they have highlighted different open issues and research challenges that are faced in smart healthcare systems.Chamola et al.[3] proposed an AI-assisted blockchain-based framework in which the medical records (handwritten prescriptions, printed prescriptions, and printed reports) are stored and processed using various AI techniques like optical character recognition (OCR) to form a single patient medical history report. The report concisely presented only the crucial information for convenience and is stored securely over a decentralized blockchain network for later use.

Aich etal.[4] presented a solution based on blockchain and AI technologies. The blockchain will securely protect the data access and AI-based federated learning for building a robust model for global and real-time usageTanget al. [5] proposed a secure and trusted collaborative learning framework called TrusCL. The framework guarantees privacy preservation via a delicate combination of homomorphic encryption (HE) and differential privacy (DP), achieving the trade-off between efficiency and accuracy. Furthermore, based on blockchain, in their design, the key steps of secure collaborative learning are recorded on blockchain so that malicious behaviors can be effectively tracked and choked in a timely manner to facilitate trusted computation. Experimental results validate the trade-off performance of Trus-CL between model training efficiency and trained model accuracy.

Haddadet al. [6] proposed a system which was used to conduct a Systematic Literature Review (SLR) to identify and assess research articles that were either conceptual or implemented to manage EHRs using blockchain technology.Panwar et al. [7] proposed a novel framework for personal health record (PHR) management using IBM cloud data lake and blockchain platform for an effective healthcare management process. The problem in the blockchain-based healthcare management system can be minimized with the utilization of the proposed technique. Significantly, the traditional blockchain system usually decreases the latency. Therefore, the proposed technique focused on improving latency and throughput. The result of the proposed system is calculated based on various matrices, such as F1 Score, Recall, and Confusion matrices. Therefore, the proposed work scored high accuracy and provided better results than existing techniques.

Nicolas et al.[8] proposed a solution that allows providers to share their data and run their algorithms in secured cloud training environments. To provide trust for both clients and asset providers in the system, a blockchain was introduced to support the negotiation, monitoring, and conclusion of model production. Through a preliminary evaluation, they have validated the feasibility of the approach and presented a road map to a more secure Artificial Intelligence as-a-service.Rana et al.[9] proposed a decentralized access control modelwhich enable the secure interoperability of different healthcare organizations. That model used the Ethereum blockchain for its implementation. That model interfaces patients, doctors, chemists, and insurance companies, empowering the consistent and secure exchange of data. The major concerns are maintaining a history of the transactions and avoiding unauthorized updates in health records. Any transaction that changes the state of the data is reflected in the distributed ledger and can be easily traced with that model. Only authorized entities can access their respective data. Even the administrator will not be able to modify any medical records.

Adelet al. [10] proposed a system which was developed as an inference engine while having a number of interesting features. First, the system validates and audits the decision-making process while sharing and recording the input data and the computed outcomes in a synchronized trusted manner. Second, the system allows the formation of distributed AI repository that can absorb and manage concurrent use-cases while targeting different scopes and covering diverse AI branches. Third, it provides a workable solution for the AI applications' distribution problem, which hinders their wide employment. Fourth, the introduced system guarantees sustainable versioning and evolution over time for AI applications based on their performance or the newly acquired data.

Sujatha et al. [11] proposed Secretary Network, that will keep data safe, computer programming, and sharing within the Internet environment, aimed at a real cyber safe real estate data and thus improve AI with multiple data sources, with to combine three key elements: Block proprietary data sharing guarantee, which allows for reliable data sharing within a large area to make real big data; Creating a reliable cyberspace, based on AI a secure computer platform is used for mass production smart safety rules. A reliable way to exchange the purchase price Security, they provide the way participants have seen economic rewards when releasing their data or service, which encouraged the sharing of information and thus achieved better AI performance. Moreover, they talked standard usage of Sec Net and its another possible method, as well as analysis its effectiveness from the aspect of network security and economic revenue.

Suryavanshi et al. [12] proposed a Blockchain and AI empowered framework. The future of technology was driven by the power of blockchain, AI, and web 3.0, providing a secure and efficient way to manage digital assets and data.Vrushank et al. [13] proposeda architecture that used proxy re-encryption mechanisms and IPFS with Arweave to enhance the privacy, immutability, and permanence of the data.Rajawat et al. [14] proposed AI and Blockchain based framework for improving the data security in the smart cities domain.Rabieinejad et al.[15]proposed a secure framework using blockchain and Deep Neural networks (DNN) to address the challenges. In that framework, they have considered cluster-based architecture that vehicles in each cluster can securely communicate using the blockchain. Also, DNN was adopted to detect abnormal vehicles that have been attacked using their network traffic analysis in each zone.

3. PROPOSED METHOD

1 Overview

The system utilizes a combination of blockchain technology and artificial intelligence (AI) to secure medical data. Blockchain, a distributed ledger technology, ensures the integrity and immutability of data by creating a chain of blocks containing transactional records. AI algorithms enhance the security of the blockchain network by employing advanced cryptographic techniques and consensus mechanisms.

- **Django Framework Setup:**The code has configurations for a Django web framework, which is a high-level Python web framework known for its simplicity and scalability. It simplifies the creation of web applications by providing built-in features for authentication, URL routing, and database management.
- **Block Class Implementation:** A **Block** class represents a single block in the blockchain. Each block contains an index, a list of transactions, a timestamp, a previous hash, and a nonce value. The **compute_hash()** method calculates the hash of the block using the SHA-256 hashing algorithm.
- **Blockchain Class Implementation:** The **Blockchain** class manages the blockchain network and consists of methods for adding blocks, mining new blocks, and validating transactions. It maintains a chain of blocks and implements a proof-of-work (PoW) algorithm to achieve consensus among network participants.
- **Proof-of-Work Algorithm:** The PoW algorithm requires miners to solve complex mathematical puzzles to add new blocks to the blockchain. Miners iterate through nonce values until they find a hash that meets the specified difficulty criteria, which involves leading zeros in the hash. This process ensures the security and integrity of the blockchain by making it computationally expensive to alter transaction history.
- **Django Views and URL Configuration:** The Django views and URL configuration define the endpoints and functionalities of the web application. These components handle user requests, process data, and render dynamic web pages. The URLs map to specific views, which interact with the blockchain backend to perform operations such as creating profiles, accessing medical data, and authenticating users.
- **Integration of Blockchain with Django:** The blockchain functionalities are integrated into the Django web application to secure medical data and ensure data privacy. By leveraging blockchain technology, the system provides a decentralized and tamper-proof storage solution for sensitive medical records. AI algorithms can further enhance security by detecting anomalies, preventing unauthorized access, and encrypting data.

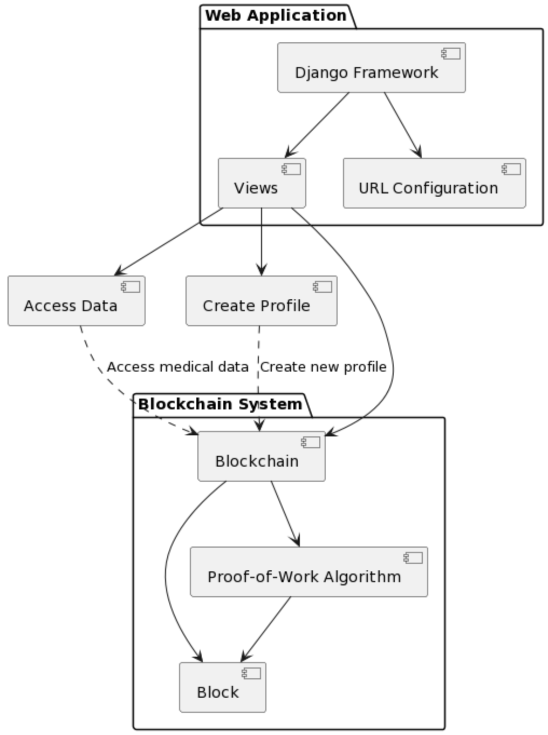

Figure 1: Block Diagram of proposed System.

2 Database

The SQL code is used to create a database named "SecuringData" and define a table named "patients" within it. This table structure is designed to store patient-related information securely, including personal details, medical history, access permissions, and blockchain hash values for data integrity verification. It provides a foundation for managing and securing medical data within the "SecuringData" database.

Let's break down the table structure and explain each field:

- **Patient_id** (int): This field represents the unique identifier for each patient. It is of integer type, typically used as a primary key to uniquely identify each record in the table.
- **patient_name** (varchar(50)): This field stores the name of the patient. It is of variable character type with a maximum length of 50 characters.
- **age** (int): This field stores the age of the patient. It is of integer type.
- **problem_desc** (varchar (500)): This field stores a description of the medical problem or condition faced by the patient. It is of variable character type with a maximum length of 500 characters.
- **profile_date** (date): This field stores the date when the patient's profile was created or last updated. It is of date type.

- **access_data** (varchar (200)): This field stores information related to the access rights or permissions for the patient's data. It is of variable character type with a maximum length of 200 characters.
- **gender** (varchar (30)): This field stores the gender of the patient. It is of variable character type with a maximum length of 30 characters.
- **contact_no** (varchar (12)): This field stores the contact number of the patient. It is of variable character type with a maximum length of 12 characters.
- **address** (varchar (100)): This field stores the address of the patient. It is of variable character type with a maximum length of 100 characters.
- **blockchain_hash** (varchar (200)): This field stores the hash value associated with the patient's data in the blockchain. It is of variable character type with a maximum length of 200 characters, indicating a hash value generated using cryptographic algorithms.
- **revenue** (double): This field stores revenue-related information associated with the patient, such as billing or financial transactions. It is of double precision floating-point type.

4. Results and Description

Figure 1 depicts the home screen of an application designed for securing medical data. This screen serves as the entry point for users, providing them with options to navigate through the app's functionalities. It includes features such as login, registration, and access to various sections like patient profiles, hospital databases, or administrative tools.

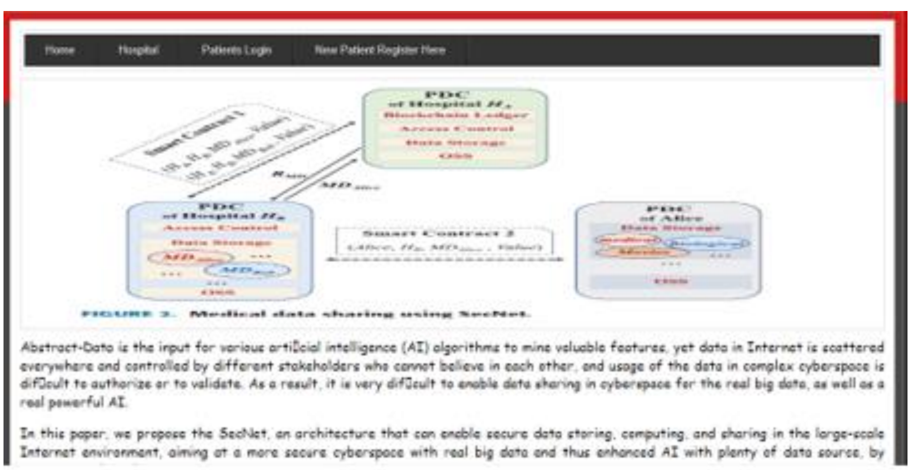

Figure 1: Home Screen of Securing Medical Data.

Figure 2, users are shown entering patient details to create a profile. This step is crucial for accurately storing and accessing medical records. It typically involves inputting information such as name, date of birth, medical history, and contact details. Creating a profile ensures that patient data is organized and easily retrievable when needed.

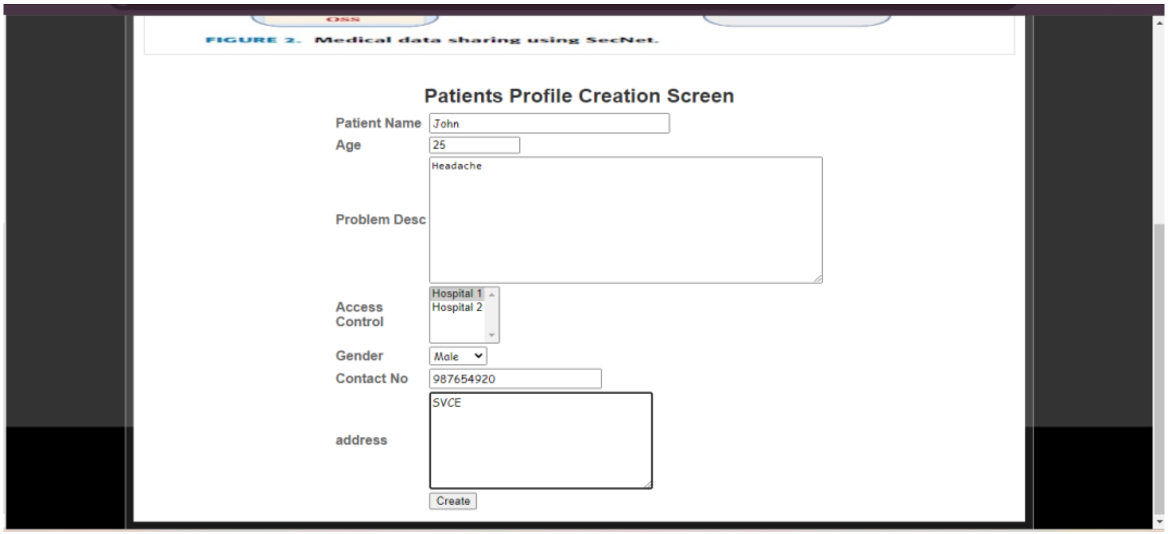

Figure 2: entering patient details for Profile Creation.

Figure 3 displays the login screen specifically designed for hospital personnel. This screen prompts users to enter their credentials, typically a username and password, to access the hospital's database or administrative features. Hospital staff may use this login to update patient records, schedule appointments, or access medical imaging systems.

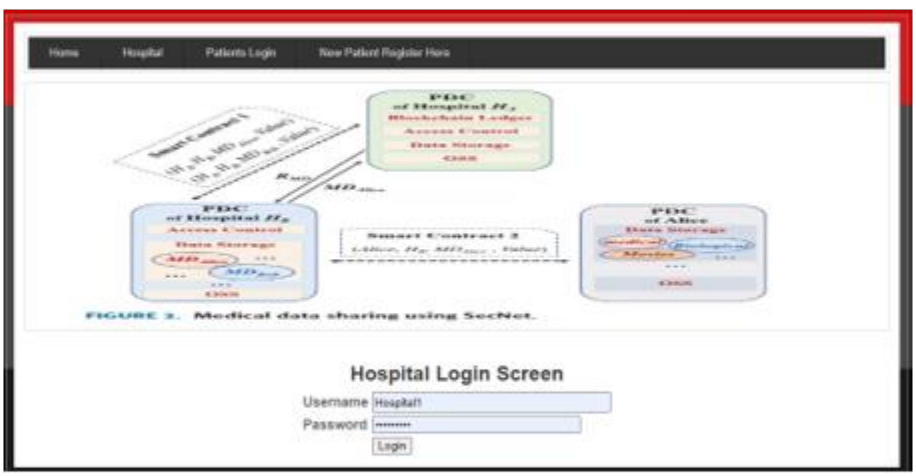

Figure 3: Hospital Login Screen

Figure 4 shows the screen where authorized users can access patient details. Once logged in, hospital staff can search for specific patients and view their medical records. This screen display information such as diagnosis, treatment history, lab results, and medication prescriptions.

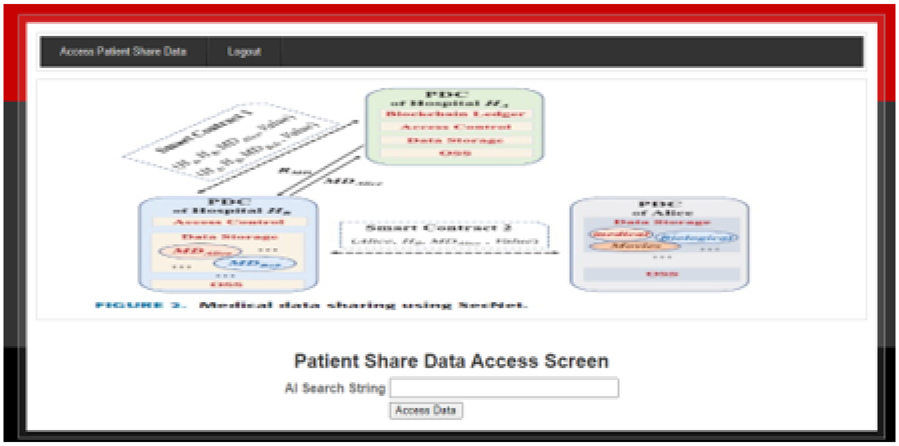

Figure 4: Patient details Access Screen

In Figure 5, the patient details screen is displayed, providing a comprehensive overview of the selected patient's medical information. This screen include tabs or sections for different aspects of the patient's health, allowing hospital staff to navigate through their records efficiently.

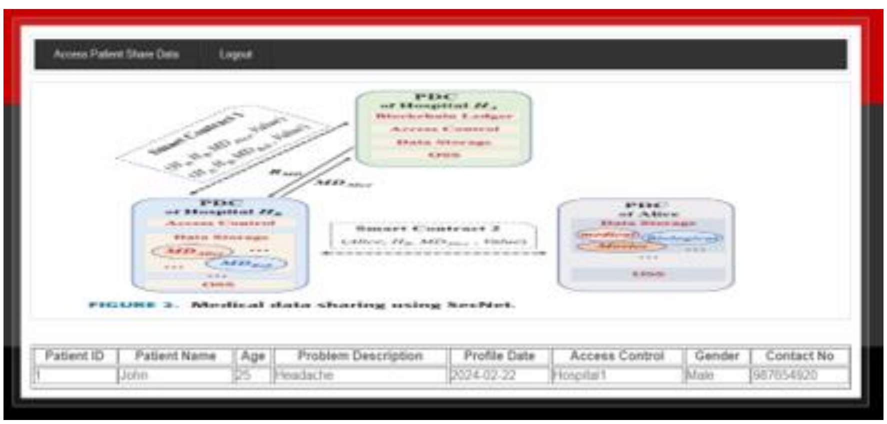

Figure 5: Display patient details screen

Figure 6 presents the login screen for patients themselves. Patients can log in to access their own medical records, review upcoming appointments, or communicate with their healthcare providers. Patient login screens often prioritize user-friendly interfaces and may include features like password recovery options or biometric authentication.

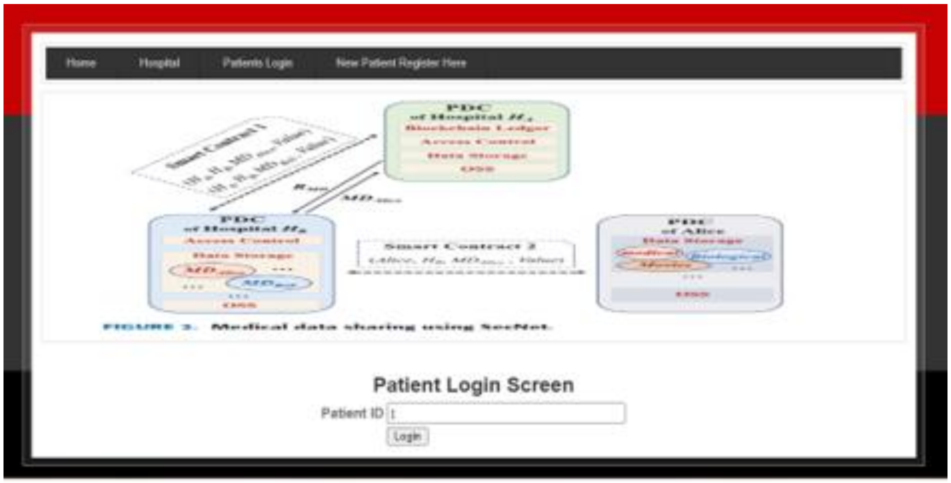

Figure 6: Patient login Screen.

Figure 7 displays the patient details along with its associated blockchain hash code. This screen provides an additional layer of security by leveraging blockchain technology to encrypt and authenticate patient data. Each patient record is assigned a unique hash code, ensuring the integrity and confidentiality of their medical information.

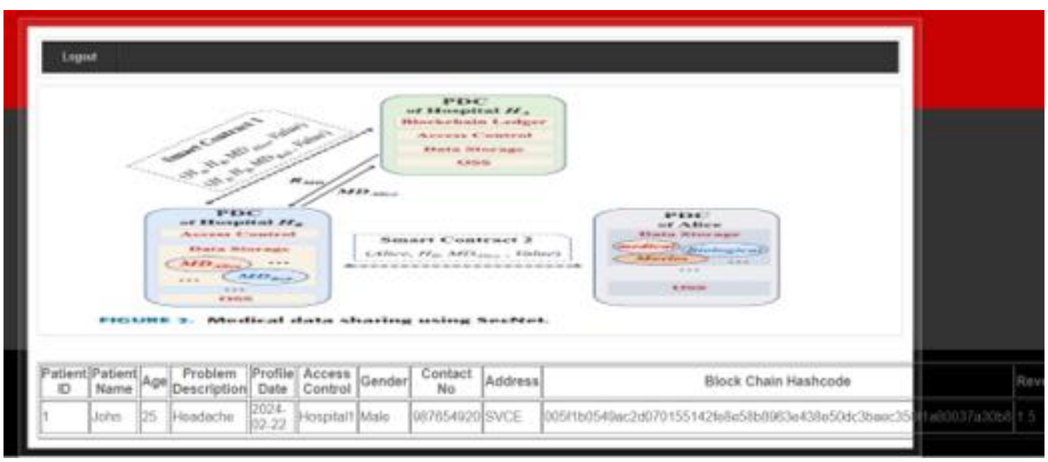

Figure 7: Displays Patient details of Patient and its Block Chain Hash Code.

5. CONCLUSION

The integration of blockchain technology into AI applications offers a promising avenue for enhancing data security and integrity in an increasingly interconnected digital landscape. By leveraging blockchain's inherent characteristics of immutability, decentralization, and cryptographic security, organizations can establish trust and transparency in data transactions, ensuring the integrity and authenticity of information exchanged within AI systems. Through the use of smart contracts, blockchain facilitates automated and tamper-proof execution of agreements, providing a robust framework for governing data access and usage permissions. Additionally, blockchain's distributed ledger architecture mitigates the risk of single points of failure and unauthorized tampering, thereby bolstering the resilience of AI systems against malicious attacks and data breaches. As AI continues to play an increasingly vital role in various domains, from healthcare and finance to supply chain management and cybersecurity, the integration of blockchain technology serves as a crucial enabler for fostering trust, accountability, and security in data-driven decision-making processes. Embracing this synergy between blockchain and AI holds the potential to unlock new opportunities for innovation while safeguarding sensitive data and preserving privacy rights in the digital age.

REFERENCES

[1] Rajawat, Anand Singh, Pradeep Bedi, S. B. Goyal, Rabindra Nath Shaw, Ankush Ghosh, and Sambhav Aggarwal. "Ai and blockchain for healthcare data security in smart cities." *AI and IoT for Smart City Applications* (2022): 185-198.

[2] Alabdulatif, Abdulatif, Ibrahim Khalil, and Mohammad Saidur Rahman. "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis." *Applied Sciences* 12, no. 21 (2022): 11039.

[3] Chamola, Vinay, Adit Goyal, Pranab Sharma, Vikas Hassija, Huynh Thi Thanh Binh, and Vikas Saxena. "Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management." *Neural Computing and Applications* 35, no. 31 (2023): 22959-22969.

[4] Aich, Satyabrata, Nday Kabulo Sinai, Saurabh Kumar, Mohammed Ali, Yu Ran Choi, Moon-IL Joo, and Hee-Cheol Kim. "Protecting personal healthcare record using blockchain & federated learning technologies." In *2022 24th International Conference on Advanced Communication Technology (ICACT)*, pp. 109-112. IEEE, 2022.

[5] Tang, Xiangyun, Liehuang Zhu, Meng Shen, Jialiang Peng, Jiawen Kang, Dusit Niyato, and Ahmed A. Abd El-Latif. "Secure and trusted collaborative learning based on blockchain for artificial intelligence of things." *IEEE Wireless Communications* 29, no. 3 (2022): 14-22.

[6] Haddad, Alaa, Mohamed Hadi Habaebi, Md Rafiqul Islam, Nurul Fadzlin Hasbullah, and Suriza Ahmad Zabidi. "Systematic review on ai-blockchain based e-healthcare records management systems." *IEEE Access* 10 (2022): 94583-94615.

[7] Panwar, Arvind, Vishal Bhatnagar, Manju Khari, Ahmad Waleed Salehi, and Gaurav Gupta. "A blockchain framework to secure personal health record (phr) in ibm cloud-based data lake." *Computational Intelligence and Neuroscience* 2022 (2022).

[8] Six, Nicolas, Andrea Perrichon-Chrétien, and Nicolas Herbaut. "Saiaas: A blockchain-based solution for secure artificial intelligence as-a-service." In *The International Conference on Deep Learning, Big Data and Blockchain (Deep-BDB 2021)*, pp. 67-74. Springer International Publishing, 2022.

[9] Rana, Sumit Kumar, Sanjeev Kumar Rana, Kashif Nisar, Ag Asri Ag Ibrahim, Arun Kumar Rana, Nitin Goyal, and Paras Chawla. "Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare." *Sustainability* 14, no. 15 (2022): 9471.

[10] Adel, Kareem, Ahmed Elhakeem, and Mohamed Marzouk. "Decentralizing construction AI applications using blockchain technology." *Expert Systems with Applications* 194 (2022): 116548.

[11] Sujatha, B., K. Anas Faraz, N. Pranathi, Ch BR Saranya, and B. S. V. Chaitanya. "Securing data with blockchain and AI." In *AIP Conference Proceedings*, vol. 2492, no. 1. AIP Publishing, 2023.

[12] Suryavanshi, Akshay, G. Apoorva, Mohan Babu TN, M. Rishika, and Abdul Haq. "The integration of Blockchain and AI for Web 3.0: A security Perspective." In *2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT)*, pp. 1-8. IEEE, 2023.

[13] Shah, Vrushank, Vidhi Thakkar, and Alex Khang. "Electronic health records security and privacy enhancement using blockchain technology." In *Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem*, pp. 1-13. CRC Press, 2023.

[14] Rajawat, Anand Singh, Pradeep Bedi, S. B. Goyal, Rabindra Nath Shaw, Ankush Ghosh, and Sambhav Aggarwal. "Ai and blockchain for healthcare data security in smart cities." *AI and IoT for Smart City Applications* (2022): 185-198.

[15] Rabieinejad, Elnaz, Abbas Yazdinejad, Ali Dehghantanha, Reza M. Parizi, and Gautam Srivastava. "Secure ai and blockchain-enabled framework in smart vehicular networks." In *2021 IEEE Globecom Workshops (GC Wkshps)*, pp. 1-6. IEEE, 2021.