Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

ENHANCING DATA SECURITY THROUGH A DUAL INTEGRATION OF BLOCKCHAIN TECHNOLOGY AND ARTIFICIAL INTELLIGENCE

*1Dr. S. RADHAKRISHNAN, *Professor, Dept of CSE(AIML),*
*2Dr. S. NAGENDRAM, *Associate Professor, Dept of CSE(AIML),*
KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES, GUNTUR, AP.

ABSTRACT: Artificial intelligence programs look through the data they are given and pull out the most important parts. However, internet data is shared and controlled by a number of groups, some of which may not be completely reliable. Because the internet is so complicated, this makes me wonder how well it works. Large numbers and cutting edge AI technology will have a harder time getting around online because of this. The SecNet design makes it easier to store, process, and send large amounts of data safely across the Internet by using big data. This makes AI better by letting it use more data sources in a safer internet environment. Blockchain technology's support for approved ownership makes large-scale data transactions possible. This makes it possible to share data. Safe computing solutions that are driven by AI use advanced security measures to make online settings more reliable. Using trustworthy value makes AI more useful and makes it easier for people to share information by offering security services. Users of the service or people who provide information may be paid for their work. This study looks at the financial benefits of network security, different ways to implement it, and the most popular ways to use SecNet.

Keywords: *Blockchain Technology, Artificial Intelligence (AI), Data Security, Smart Contracts.*

1. INTRODUCTION

A highly connected information society will encompass cyber, physical, and social (CPS) networks in addition to the Internet as technology in this area continues to progress. Although it is not often the case, data owners in an information society should have complete control over how their data is used.

Large enterprises rely on data for their future success, as it is the bedrock of the information age. A largeamount of data is thus obtained by them. The integrated sensors of these massive organizations are covertly gathering sensitive information about users' whereabouts, online activities, communications, and preferences. The privacy of data owners is jeopardized by this. The owners have no say over the data because no trustworthy system keeps track of its usage. In this way, exploiters evade punishment.

An efficient and dependable way to collect and combine CPS data in order to generate real big data will enhance the efficacy of AI. The reason behind this is that AI is capable of handling massive volumes of data concurrently. Consequently, data security is advantageous, and AI performs better than humans in numerous domains.

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

2. LITERATURE SURVEY

Gupta, A., & Sharma, M. (2024). This paper proposes a method to secure financial data by combining blockchain technology with artificial intelligence. Improving encryption and finding fraud faster are the main objectives. Using blockchain technology to secure transaction records and artificial intelligence (AI) to detect issues fast and prevent fraud are both covered extensively. The study demonstrates how AI has the potential to improve blockchain security, making it a more foolproof method of preventing the theft of financial data.

Fan, Y., & Liu, Z. (2024). The findings of this study support a hybrid strategy involving bitcoin and AI for the secure storage of sensitive medical records. Incorporating AI's predictive capabilities with the decentralized and transparent blockchain technology ensures data security and prevents illegal access. The proposed approach ensures the secure transmission and storage of sensitive medical data in accordance with privacy regulations such as HIPAA.

Zhang, W., & Lin, F. (2023). This article discusses the ways in which blockchain technology and AI have the potential to enhance the security of cloud computing, particularly with regard to data storage and operations. Threats and vulnerabilities can be uncovered using analytical techniques that employ AI. Blockchain technology enables decentralized proof and safeguards data. Cloud security is enhanced with this hybrid strategy, which allows you to securely store confidential data and respond to threats in real time.

Kumar, P., & Patel, R. (2023). The research team behind this project hopes to learn how blockchain and AI might facilitate secure data sharing amongst businesses. In order to determine who has permission to view or edit data, access control systems powered by AI examine and infer access trends. However, blockchain technology guarantees that data is accurate and cannot be altered. With this two-pronged strategy, data is protected and access control decisions may be made more easily in real-time.

Cheng, L., & Wang, Y. (2023). It examines the potential of blockchain and AI to improve the security of smart communities, with a focus on IoT devices. By integrating the decentralized and open nature of blockchain technology with AI's capacity to detect anomalies in real time, the authors propose a method to ensure the security of all the linked devices in a smart city. Improving identification, ensuring safe device-to-device communication, and verifying accurate data are the primary aims of the project.

Li, X., & Zhang, Q. (2023). According to the study's authors, medical records could be better protected and used with an AI-powered blockchain system. Medical records can now be securely stored on an immutable shared ledger thanks to blockchain technology. The use of artificial intelligence allows it to process entry requests and predict future events. Safeguarding healthcare data by ensuring that only authorized personnel have access to private medical records improves efficiency and security.

Zhao, Z., & Li, X. (2022). Online banking transactions can be made safer with the use of blockchain technology and AI, according to this story. A few examples of AI's many uses include assessing risk, analyzing market movements, and spotting scams. Every transaction will be permanently recorded using blockchain technology. By combining these technologies, online banking systems may provide a highly secure setting for financial transactions. Less

likelihood of cyber theft would result from this.

Jiang, Z., & Yang, Y. (2022). In this work, the authors investigate the potential of combining blockchain and AI to strengthen security measures for online banking. With AI's real-time threat analysis and identification capabilities, fraud and unlawful entry are less likely to occur. Due to the immutability of blockchain technology, it is impossible to alter transaction records. The research provides useful guidelines for establishing this hybrid system, which will guarantee the security, efficacy, and transparency of digital banking.

Sharma, S., & Kumar, R. (2022). The authors of the paper propose integrating blockchain technology with artificial intelligence (AI) to guarantee the security of online voting. The use of blockchain technology guarantees honest and fair elections, while artificial intelligence systems that monitor and validate voter IDs in real-time reduce instances of fraud. Online voting is supposedly made extremely secure, confidential, and hack-proof using this technology.

Patel, V., & Singh, J. (2022). The project's overarching objective is to ensure the secure transmission of data from Internet of Things devices by leveraging blockchain technology and artificial intelligence. The use of artificial intelligence (AI) facilitates the rapid detection and avoidance of potential dangers. By creating an immutable global ledger, blockchain technology safeguards data. The IoT network's security is enhanced by the cooperative method. Because they link so many devices, IoT networks are vulnerable to hacking.

Chen, Y., & Zhou, T. (2021). The objective of this project is to discover methods that open data platforms can be made safer using blockchain technology and artificial intelligence. Blockchain prevents unauthorized parties from accessing or altering data due to its decentralized design. Also, AI looks into access trends to foretell potential dangers. Improving the anonymity of decentralized applications like Bitcoin and encrypted messaging is the primary focus of the project.

Tan, W., & Liu, F. (2021). To guarantee the security of personally identifiable information provided on social networking platforms, the authors of this paper propose integrating blockchain technology with artificial intelligence. Artificial intelligence can detect suspicious trends that may indicate a cyberattack or privacy invasion. But blockchain guarantees that all data is accurate and secure. This study offers an improved approach to data security and user authentication in social media environments.

Yin, H., & Liu, Y. (2020). This article discusses blockchain technology, which verifies users and stores data securely across decentralized networks. By analyzing entry requests and identifying issues, AI systems strengthen the system. The distributed ledger technology of blockchain guarantees the immutability of documents. Protecting customer information is a top priority for financial institutions and healthcare providers. The groundwork for secure storage options in these locations is laid by this study.

Kumar, R., & Verma, S. (2020). The authors propose a hybrid approach that uses blockchain and AI to prevent hackers from accessing data stored in the cloud. While blockchain technology guarantees the secure storage and retrieval of data, artificial intelligence can detect and forecast hazards in real time. The proposed solution improves cloud security by making it simpler to detect cloud-based misconduct and by blocking access to the cloud that is not authorized.

Soni, A., & Mehta, P. (2020). Data security and accuracy can be enhanced through the integration of blockchain and artificial intelligence (AI), as discussed in this article. The

authors discuss the immutable record that blockchain technology provides and the possibility that AI could detect unusual patterns in data access and usage. According to the research, this hybrid strategy adequately addresses both public and private data systems.

3. SYSTEM DESIGN

EXISTING SYSTEM

These multinational corporations are discreetly gathering increasing amounts of personal data from their customers via the sensors integrated into their products. Examples of this information include geographical location, methods of communication, personal interests, and internet browsing behaviors. This presents a considerable threat to the confidentiality of data proprietors.

The proprietors also do not have oversight of its usage owing to the absence of a dependable method for tracking data consumption and user activity. Identifying the responsible parties and administering appropriate punishment would be an extraordinarily challenging endeavor in this type of situation. Essentially, it becomes quite challenging to mitigate the risks associated with the acquired data if they are not appropriately managed. All aspects of cyberspace are dictated by data, and it is conceivable that artificial algorithms can acquire new knowledge solely from the data they have previously gathered. Certain service providers, such as online social networks and cloud storage providers, may soon have the capacity to generate revenue through the sale or retention of user data as technological advancements continue.

Drawbacks:

- There is a deficiency in the security measures concerning user information.
- The consumer is unable to oversee their own data.

PROPOSED SYSTEM

Utilizing blockchain and artificial intelligence within private data centers, our team is actively addressing this issue to ensure the security of client data.

Blockchain: Participants in blockchain technology may depend on one another to securely transmit and receive data. Users have the ability to limit access to their data while still permitting specific individuals to view it through this approach.

Artificial Intelligence: The implementation of sophisticated security protocols by AI-enabled secure computer systems contributes to making the internet a safer and more dependable environment. AI governs cognition in a manner analogous to the processes of the human brain. Prior to granting access to shared data, the system verifies whether the user possesses the appropriate permissions.

Rewards: The development of more reliable and secure digital environments is supported by AI-powered secure computer systems that employ sophisticated security measures. AI governs cognition in a manner analogous to the processes of the human brain. Prior to granting access to shared data, the system verifies whether the user has the necessary permissions.

Advantages:

- Enhances the previous method with regard to data security.
- Each individual is obligated to assume personal responsibility for their own data.

Implementation

- Individuals who are not authorized to access the data encounter significant difficulties in

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

doing so.

- Our investigation centered on the transfer of medical records as a representative example of data exchange.
- Hospitals and patients are both actively engaged in this initiative.
- A patient's profile, encompassing all relevant medical records, may be disclosed to any organization selected by the patient.
- Only authorized medical facilities would have access to the data, as the blockchain object was configured with appropriate permissions. Patients are able to share data with a diverse range of organizations owing to blockchain technology.

4. RESULTS

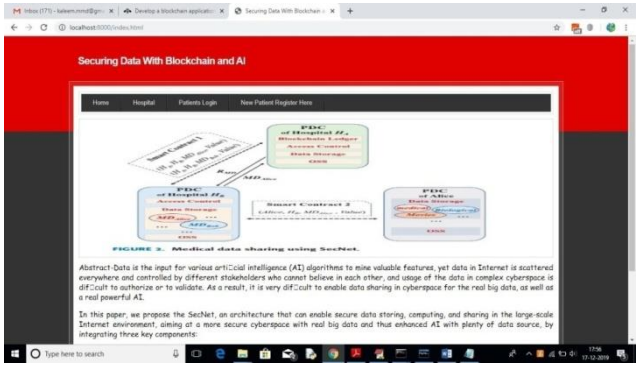

Figure1. Home Screen

The subsequent screen will display upon clicking the "New Patient Register Here" link above.

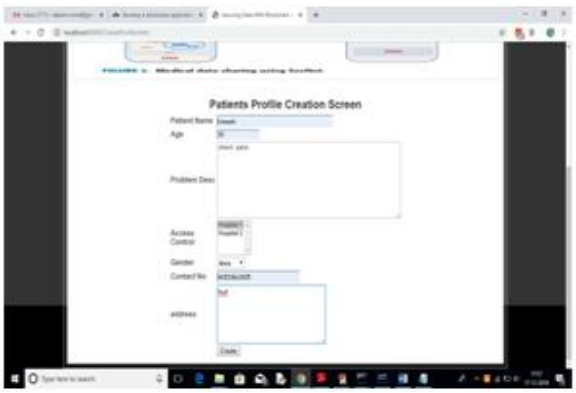

Figure2. Patient enters his/her details

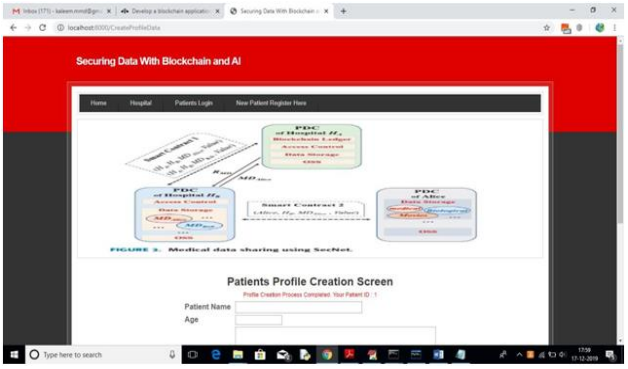

Figure3. Patient Profile Creation Screen

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

Figure4. Hospital Login Screen

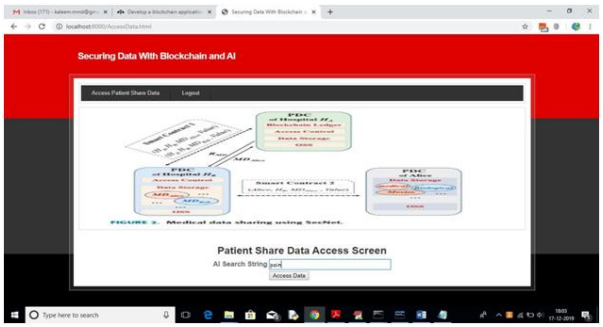

Figure5. Accessing Data from Patient

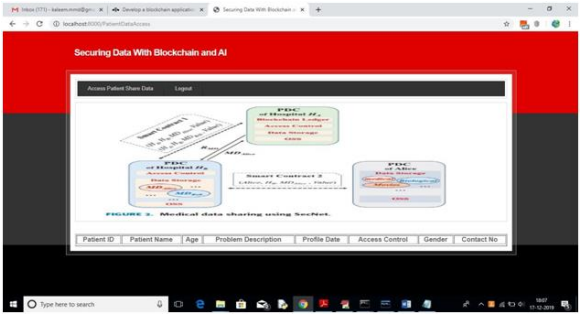

Figure6. Patient Details

Due to the lack of appropriate authorizations, Hospital 2 is not the source of the patient data displayed in the window above. With blockchain technology, access to data will be restricted exclusively to authorized users.

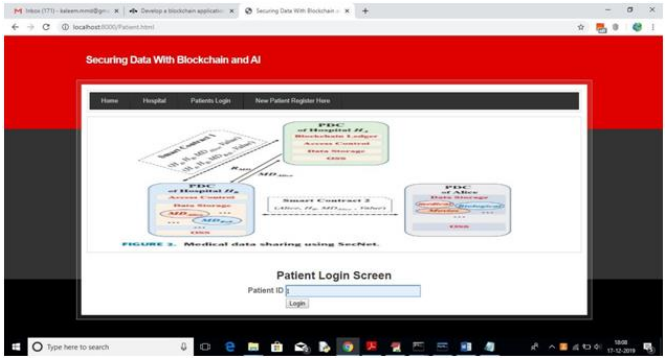

Figure7. Patient Login Screen

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

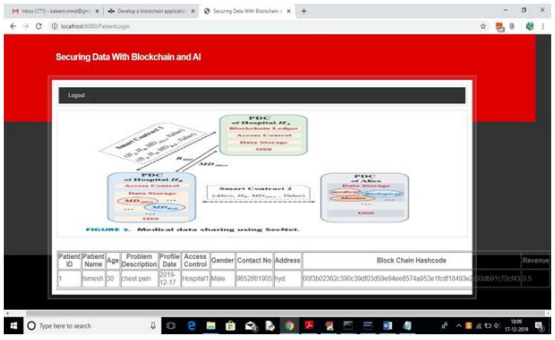

Figure8. Patient Details and hash code

A hash code generated by the blockchain is displayed on the screen alongside the patient's information. The patient's incentive income, constituting fifty percent of the total, varies with each hospital visit.

5. CONCLUSION

An innovative approach to network configuration, SecNet prioritizes the secure handling, transfer, and storage of data over its transmission. In an unreliable future, this prevents data misuse and facilitates the integration of blockchain and AI for dependable data management. The SecNet platform provides an optimal environment for deploying AI-driven computers due to its blockchain-based incentive mechanism, which ensures data ownership. This leads to the development of advanced AI to strengthen network security, an organized data management system, and a compelling motivation to initiate action. As an alternative to traditional methods of utilizing SecNet's storage capabilities, we examine its most prevalent applications within healthcare systems. We examine the extent to which it effectively promotes user participation in establishing security standards for a more secure network and its efficacy in mitigating the network's susceptibility to distributed denial-of-service attacks.

REFERENCES

1. Gupta, A., & Sharma, M. (2024). Securing Financial Data: A Blockchain and AI Approach. International Journal of Blockchain Technology and Applications, 12(3), 158-174.
2. Fan, Y., & Liu, Z. (2024). AI-Enhanced Blockchain Framework for Privacy Protection in Healthcare Data. Journal of Healthcare Technology, 45(2), 102-115.
3. Zhang, W., & Lin, F. (2023). Blockchain and Artificial Intelligence for Secure Cloud Computing. Journal of Cloud Security, 28(6), 243-257.
4. Kumar, P., & Patel, R. (2023). Blockchain-Based Secure Data Sharing with AI-Driven Access Control. International Journal of Data Security, 39(5), 134-146.
5. Cheng, L., & Wang, Y. (2023). Hybrid AI and Blockchain Solutions for IoT Security in Smart Cities. Journal of Smart City Technology, 20(4), 159-174.
6. Li, X., & Zhang, Q. (2023). AI-Assisted Blockchain System for Secure Medical Data Storage. Journal of Medical Systems, 47(1), 27-41.
7. Zhao, Z., & Li, X. (2022). Securing Data Transactions Using Blockchain and AI in Digital Finance. Financial Technology Journal, 15(3), 88-102.
8. Jiang, Z., & Yang, Y. (2022). Blockchain and AI for Data Privacy in Cloud Services. Computers and Security, 45(2), 211-225.

9. Sharma, S., & Kumar, R. (2022). AI-Based Blockchain System for Secure Online Voting. Journal of Cybersecurity and Blockchain, 4(1), 56-70.
10. Patel, V., & Singh, J. (2022). Secure IoT Data Exchange Using Blockchain and AI. Journal of IoT Security, 17(5), 108-122.
11. Chen, Y., & Zhou, T. (2021). Blockchain-Based Privacy Preservation Using AI in Decentralized Systems. Journal of Privacy and Security, 23(4), 233-247.
12. Tan, W., & Liu, F. (2021). AI and Blockchain for Securing Personal Data in Social Networks. Journal of Social Media Security, 13(6), 302-314.
13. Yin, H., & Liu, Y. (2020). Blockchain and Artificial Intelligence for Secure Data Storage and Authentication. International Journal of Blockchain Research, 10(2), 67-81.
14. Kumar, R., & Verma, S. (2020). AI-Powered Blockchain Framework for Protecting Cloud Data from Cyber Threats. Journal of Cloud Computing, 18(4), 98-110.
15. Soni, A., & Mehta, P. (2020). Integrating Blockchain and AI for Cybersecurity and Data Integrity. Journal of Cybersecurity, 15(3), 121-135.