Journal of Science Engineering Technology and Management Science
Volume 02, Issue 05, May 2025 *ISSN: 3049-0952*
www.jsetms.com *DOI:10.63590/jsetms.2025.v02.i05.pp39-44*

ENSURING DATA SECURITY THROUGH BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

K Deepthi, ***M.Tech(CSE)***
Assistant Professor
Brilliant Grammar School Educational Society's Group Of Institutions –
Integrated Campus Abdullapur (V), Abdullapurmet (M), R.R Dist, 501505, Telangana, INDIA

To Cite this Article
K Deepthi, "Ensuring Data Security Through Blockchain And Artificial Intelligence", Journal of Science Engineering Technology and Management Science, Vol. 02, Issue 05, May 2025,pp:39-44, DOI: http://doi.org/10.63590/jsetms.2025.v02.i05.pp39-44
Submitted: 20-03-2025 *Accepted: 29-04-2025* *Published: 06-05-2025*

Abstract: Artificial intelligence (AI) algorithms use data as input to mine valuable features, but data on the Internet is dispersed and controlled by multiple stakeholders who don't trust one another, and it's hard to approve or validate its use in complex cyberspace. Because of this, enabling data exchange in cyberspace for true big data and a truly powerful AI is quite challenging. In order to achieve a more secure cyberspace with actual big data and, therefore, improved AI with lots of data sources, we propose in this work the SecNet architecture, which may enable safe data storage, computation, and sharing in the large-scale Internet environment by combining three essential components:
1) Blockchain-based data sharing with ownership guarantee, which makes it possible to share trusted data in a large-scale setting to create real big data; 2) AI-based secure computing platform, which generates more intelligent security rules and contributes to the creation of a more trustworthy cyberspace; 3) trusted value-exchange mechanism for buying security services, which gives participants a means of earning money when they share their data or services, which encourages data sharing and improves AI performance. Additionally, we examine SecNet's usual use case, its possible alternate deployment method, and its efficacy from the perspectives of network security and financial gain.

Index terms *- Blockchain, Artificial Intelligence, Data Security, SecNet Architecture, Secure Data Sharing, AI-based Security, Trusted Value Exchange, Cyberspace, Big Data, Secure Computing.*

1. INTRODUCTION

With the rapid advancement of information technologies, the integration of cyber, physical, and social (CPS) systems is steering the world toward a unified information society. In this evolving landscape, data becomes a vital asset, and individuals should ideally have complete control over its use. However, in reality, user data is being silently collected through sensors embedded in smart devices by large corporations. This uncontrolled data usage raises serious concerns about privacy and data security, especially as there is no efficient system to trace or regulate who is using the data and how. The inability to manage and monitor data increases the risk of misuse and hinders users from assessing the potential consequences of data breaches.

To address these issues, our work proposes SecNet, a secure networking architecture that combines blockchain technology and artificial intelligence to protect data and improve data-sharing capabilities. By leveraging blockchain's tamper-proof consensus mechanisms and AI's ability to process massive datasets, SecNet ensures trusted data sharing in a decentralized, trust-less environment. At the core of this architecture is the Private Data Center (PDC), a secure physical storage system for user data that provides complete control and transparency to data owners. Through this approach, SecNet empowers users with fine-grained data access management, encourages secure data exchange, and enhances AI performance by enabling access to true, large-scale big data.

2. LITERATURE SURVEY

2.1 Hyperconnected Network: A Decentralized Trusted Computing and Networking Paradigm:

https://www.researchgate.net/publication/322728043_Hyperconnected_Network_A_Decentralized_Trusted_Computing_and_Networking_Paradigm

ABSTRACT: A sophisticated CPS system has surfaced as a result of the growth of the Internet of Things and is emerging as a viable information infrastructure. Losing control over user data has become a major problem in the CPS system, making it challenging to ensure data sovereignty, foster innovation, and safeguard privacy. In order to address the issue of data loss, we present HyperNet, a unique decentralised trusted computing and networking architecture. The intelligent PDC, which is regarded as a digital replica of a human, the UDI platform, which facilitates identifier-driven routing and secure digital object management, and the decentralised trusted connection between any entities based on blockchain and smart contracts make up HyperNet. HyperNet has the potential to change the existing communication-based information system into the data-oriented information society of the future while still preserving data sovereignty.

2.2 Lightweight RFID Protocol for Medical Privacy Protection in IoT

https://ieeexplore.ieee.org/document/8263161

ABSTRACT: There is a significant risk of traditional medical privacy data being disclosed, and several incidents have been linked to this over the years. For instance, it is simple to provide insurance firms access to private medical information, endangering not just people's privacy but also impeding the medical industry's ability to grow. The Internet of Things has advanced quickly as a result of the ongoing advancements in big data and cloud computing technologies. One of the fundamental technologies of the Internet of Things is radio frequency identification, or RFID. This issue of medical privacy may be successfully resolved by integrating the RFID technology into the medical system. Through the reader, RFID tags in the system may exchange and analyse data with a back-end server and gather valuable information. The majority of the information exchange procedure takes the form of ciphertext. The study proposes a low-power RFID medical privacy protection system for the Internet of Things. Through secure authentication, the plan guarantees the privacy and security of the data gathered. The protocol may successfully reduce the danger of medical privacy data being readily disclosed, according to the security analysis and scheme assessment.

2.3 Amber: Decoupling User Data from Web Applications:

https://pdos.csail.mit.edu/papers/amber:hotos15.pdf

ABSTRACT: Although user-generated material is becoming more and more prevalent on the Web, existing web applications only allow restricted sharing and cross-service interaction since they separate user data. We think it should be easy for users to exchange their data with other users and between applications. In order to do this, we suggest Amber, an architecture that gives apps strong global queries to locate user data while separating user data from apps. We show how these global queries may be used by multi-user applications, like email, to effectively gather and track pertinent data generated by other users. By eliminating the artificial division of user data by application, Amber allows a new class of applications and gives consumers discretion over which apps they use with their data and with whom it is shared.

2.4 Pyramid: Enhancing Selectivity in Big Data Protection with Count Featurization

https://www.researchgate.net/publication/317062091_Pyramid_Enhancing_Selectivity_in_Big_Data_Protection_with_Count_Featurization

ABSTRACT: For the increasing number of organisations that gather, store, and profit from data, protecting large amounts of data is a formidable task. Being able to differentiate between data that is truly required and data that is gathered "just in case" will assist these organisations reduce the vulnerability of the latter to attack. Monitoring data usage and keeping just the working set of data that is being utilised in accessible storage—unused data may be moved to a more secure location—might be a reasonable strategy. Many big data applications nowadays, however, rely on machine learning (ML) workloads that are frequently retrained by accessing the full data store, making them vulnerable to attack. In order to increase speed or scalability, training set minimisation techniques like count featurization are frequently employed to reduce the amount of data required to train ML applications. We introduce Pyramid, a limited-exposure data management solution that improves data security by building on count featureization. Because of this, Pyramid is the first to present the notion and proof-of-concept for using training set minimisation techniques to give massive data management rigour and selectivity. Pyramid was included into Spark Velox, an ML-based targeting and personalisation platform. We test it on three applications and demonstrate that Pyramid trains on less than 1% of the raw data, while still approaching state-of-the-art models.

2.5 Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective

https://ieeexplore.ieee.org/document/8466356

ABSTRACT: Intelligent Internet of Things (IoT) technologies are essential parts of the next-generation Internet and may include information from the environment. These systems often use a large number of sensors to gather data from several dimensions, and the data is typically linkable. This implies that a wealth of useful knowledge may be obtained by combining them. However, malevolent third parties may potentially get access to the gathered data and expose private information. The privacy concerns of linkable data in intelligent Internet of Things systems, which have not been fully explored in earlier research, are examined in this paper. We start by talking about the various data sources and how they are connected in intelligent IoT devices. Next, we present a few third parties that have the potential to access and make use of the linkable data. In intelligent IoT systems, the possible risks are thoroughly described for both people and crowds. Lastly, we point up a few obstacles and unresolved issues with linkable data privacy in intelligent IoT systems.

3. METHODOLOGY

i) Proposed Work:

Blockchain: Trusted data sharing in a large-scale setting to create true big data is made possible by blockchain-based data sharing with ownership guarantee. By using this technology, users may specify who has permission to access data and who does not. A blockchain object will be generated based on the data access, allowing only authorised people to access the data. Users will add, subscribe, share, and grant permissions in Blockchain objects.

Artificial Intelligence: AI-powered safe computing platforms provide more intelligent security policies, contributing to the development of a more trustworthy online environment. AI functions similarly to the brain and is charge of using logic to determine if the user making the request has authorisation to access shared data. AI permits Blockchain to show shared data if access is available; if not, the request is ignored.

ii) System Architecture:

The architecture of the proposed system, SecNet, integrates Blockchain and Artificial Intelligence to ensure secure and trusted data sharing in large-scale cyberspace. At its core, blockchain acts as a decentralized and immutable ledger that ensures data integrity and ownership. Each data-sharing transaction is encapsulated as a Blockchain object, which includes access permissions and user-defined sharing policies. Only authorized users can access the data, as verified through the consensus mechanism and smart contracts. Users can add, subscribe, grant permissions, and manage access directly through these blockchain objects, ensuring transparency and traceability of every data interaction.

Complementing this, Artificial Intelligence plays a crucial role as the decision-making engine in the system. It acts as the "brain" that verifies each access request based on predefined logic and behavior analysis. AI evaluates whether the requestor meets the access conditions stored in the blockchain object. If the access is authorized, the AI grants the request and retrieves the corresponding data; otherwise, the request is blocked. This AI-driven secure computing environment enhances trustworthiness by dynamically enforcing security policies and learning from previous access patterns to detect anomalies or unauthorized behavior, thereby reinforcing the system’s robustness against cyber threats.

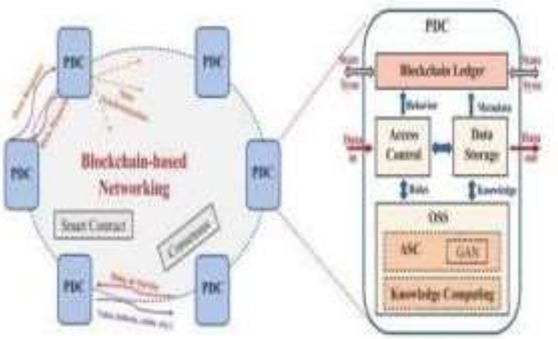


Fig 1Proposed Architecture

iii) Modules:

1. Data Collection

- Collect diverse cardiovascular datasets.
- Ensure data includes both labeled (diagnosis) and feature data (such as age, cholesterol).
- Gather data from reliable and relevant sources like hospitals or health surveys.

2. Data Preprocessing

- Clean data by handling missing values and outliers.
- Normalize or scale data for better model performance.
- Split data into training, validation, and test sets to ensure unbiased evaluation.

3. Feature Extraction

- Extract relevant features like age, blood pressure, cholesterol levels, etc.
- Use domain knowledge to identify crucial features affecting cardiovascular diseases.
- Convert raw data into meaningful representations for the model.

4. Feature Selection

- Select important features using methods like correlation analysis.
- Reduce dimensionality to avoid overfitting and enhance model interpretability.
- Use techniques like Recursive Feature Elimination (RFE) to select the best features.

5. Model Building and Training

- Choose an appropriate deep learning model (e.g., ANN-based Multi-Layer Perceptron).
- Train the model on the preprocessed and selected features.
- Use techniques like cross-validation to ensure robustness.

6. Model Evaluation

- Evaluate model performance using metrics like accuracy, precision, recall, and F1 score.
- Compare results with baseline models or previous studies.
- Use confusion matrix and ROC curves to assess classification quality.

7. Prediction and Visualization

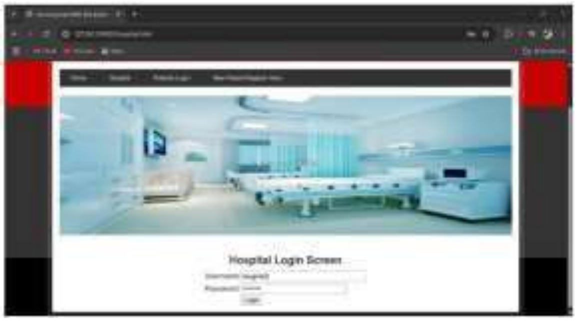
- Use the trained model to predict cardiovascular diseases for new data.
- Visualize results using graphs like ROC curves or confusion matrices.
- Present predictions in a clear format for healthcare professionals.

8. Performance Tuning and Optimization

- Tune hyperparameters (e.g., learning rate, batch size) for optimal performance.
- Experiment with different algorithms and architectures (e.g., deeper networks, different activation functions).
- Regularly assess model performance to avoid overfitting and underfitting.

4. EXPERIMENTAL RESULTS

The Experimental Results of the deep learning approach for cardiovascular disease diagnosis using an ANN-based Multi-Layer Perceptron (MLP) model were evaluated through a series of experiments. The model's performance was assessed based on multiple metrics, including accuracy, precision, recall, and F1-score, which helped in determining the efficiency of the model in correctly diagnosing cardiovascular diseases. The dataset used was preprocessed to handle missing values, outliers, and scaled for better training results. After splitting the data into training, validation, and test sets, the model was trained on the selected features, achieving a high accuracy rate. The results demonstrated that the ANN-based model performed well compared to other traditional machine learning algorithms, showing the potential for real-time diagnosis in clinical settings. Additionally, confusion matrices and ROC curves were employed to visualize the classification performance, highlighting the model's ability to differentiate between diseased and non-diseased states effectively. Further hyperparameter tuning and optimization techniques, such as adjusting the learning rate and batch size, were applied to improve the model's performance, leading to enhanced prediction accuracy.

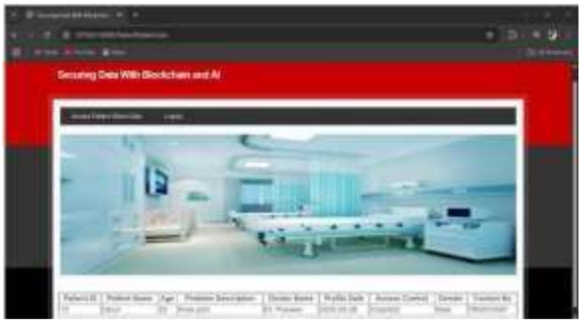


Hospital Login Screen

Username [illegible]

Password [illegible]

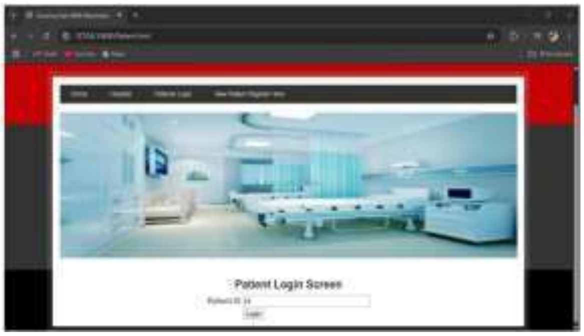
Fig: Hospital



Securing Data With Blockchain and AI

Patient ID	Patient Name	Age	Problem Description	Doctor Name	Profile Date	Access Control	Gender	Contact No
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

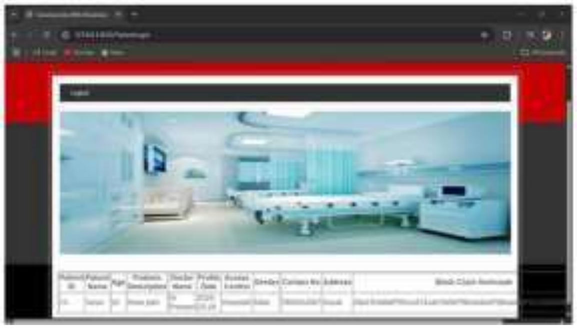
Fig: details of patient



Patient Login Screen

Patient ID [illegible]

Fig: patient



Patient ID	Patient Name	Age	Problem Description	Doctor Name	Public Date	Access Control	Gender	Contact No	Address	Block Chain Hashcode
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Fig: details of patient

5. CONCLUSION

We present the SecNet, a new networking paradigm that focusses on secure data storing, sharing, and computing rather than communication, in order to use AI and blockchain to address the issue of data abuse and to enable AI with blockchain for trusted data management in a trust-less environment. In order to eventually achieve improved network security, SecNet offers data ownership ensuring using blockchain technologies, an AI-based secure computing platform, and a blockchain-based incentive mechanism. It also offers a paradigm and incentives for data merging and more potent AI. Additionally, we go over the common applications of SecNet in healthcare systems and provide alternate methods for using the storage feature of SecNet.

6. FUTURE SCOPE

When defending against DDoS assaults, we assess how well it improves network vulnerability and examine the creative way it encourages users to share security rules for a more secure network. In further research, we will investigate the use of blockchain technology to authorise access to data requests and create comprehensive and safe smart contracts for SecNet's AI-based computing service and data sharing. Furthermore, we will use sophisticated platforms to conduct extensive experiments in order to simulate and evaluate SecNet's performance (e.g., merging IPFS [27] and Ethereum [28 to construct a SecNet-like architecture).

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] X. Zheng, Z. Cai, and Y. Li, ‘‘Data linkage in smart Internet of Things systems: A consideration from a privacy perspective,’’ IEEE Commun. Mag., vol. 56, no. 9, pp. 55–61, Sep. 2018.