

# Data Privacy using Block Chain and AI

Asst. Prof. G. Kiran Kumar, A.Hari Prasad, B. Balaraju, N. MehamoodHussain, B. Guna Sai Reddy,  
M. Jaya Kishore

Department of Computer Science and Engineering,  
SanthiramEngineering College,  
Nandyal

G. Kiran Kumar: kiran.cse@srecnandyal.edu.in

**Abstract-** While data is the fuel that drives AI algorithms, it is difficult to approve or authenticate its use in the complex internet where it resides because of its dispersed nature and the fact that its diverse stakeholders do not trust one another's stewardship. Due to this, it is challenging to facilitate data exchange in cyberspace for true big data and true powerful AI. In this paper, we propose the SecNet, an architecture that integrates three key components to enable secure data storage, computing, and sharing in the large-scale Internet environment, with the goal of creating a safer online environment rich in authentic big data and, by extension, a more robust artificial intelligence thanks to a larger pool of relevant information from which to draw. 1) Blockchain-based data sharing with ownership guarantee, allowing trustworthy data sharing in the large-scale environment to produce genuine big data. 2) An AI- based safe computing platform that may generate smarter security rules and so contribute to the development of a more reliable digital environment. As a result, greater AI performance may be attained by promoting data sharing and using a trusted value-exchange system for buying security services, which gives participants a chance to earn monetary benefits for supplying their data or service. In addition, we cover the usual deployment of SecNet and its applications.

**Keywords-** Block chain, Cryptography, smart contract, AI, SecNet.

## I. INTRODUCTION

The tendency of integrating cyber, physical, and social (CPS) systems to produce a highly cohesive information society, as opposed to just a digitized Internet, is becoming more apparent with the advancement of information technology. Data is an individual's or organization's asset in the modern information society; as such, the individual or organization should have complete say over how the data is used. As information has become the lifeblood of the modern economy, it seems to reason that major corporations would do well to amass as much data as possible.

The built-in sensors within the devices from these large firms are secretly collecting a rising quantity of personal data, including location data, web-searching activity, user calls, and user preferences, which poses a significant danger to the privacy of data owners. Furthermore, owners have limited recourse in the event of misuse of their data because of the lack of a foolproof means of tracking when and by whom the information was utilized. Since AI can handle massive amounts of data including huge information at the same time, this would bring in great benefits (e.g., achieving enhanced security for data) and even makes AI gaining the ability to exceed human capabilities in more areas if there is a efficient and trusted way to collect and merge the data scattered across the entire CPS to form real big data.

## II. RELATED WORK

**“The Hyperconnected Network: Toward a Trusted Distributed Computing and Communication Architecture,”** A sophisticated CPS system has arisen, and it's shaping up to be a very promising data backbone thanks to the rise of the Internet of Things. It is now very difficult to maintain privacy, foster innovation, and ensure data sovereignty in the CPS system due to the loss of control over user data. To address the problem of dwindling access to one's own data, we offer HyperNet, a revolutionary decentralized trustworthy computing and networking model.

HyperNet is made up of the intelligent PDC, which can be thought of as the digital clone of an individual, the decentralized trusted connection between any entities based on blockchain and smart contract, and the UDI platform, which enables secure digital object management and an identifier-driven routing mechanism. HyperNet's capacity to safeguard data sovereignty is only one of many ways in which it stands to revolutionize the information system and usher in a data-driven era of computing.

**“Protection of patient confidentiality in the Internet of Things via a lightweight RFID protocol,”** There has been a steady stream of incidents throughout the years showing just how vulnerable traditional medical privacy data really is. When sensitive information, including as

patients' medical records, leaks to insurance companies, it not only endangers patients' privacy but also stymies the industry's progress. Rapid advancements in IoT innovation have coincided with the maturation of cloud computing and big data analytics platforms.

One of the foundational technologies of the Internet of Things is radio-frequency identification (RFID). This issue of medical privacy may be efficiently addressed with the implementation of the RFID technology into the medical system. Using the reader, the system's RFID tags may capture data, which can then be sent to a back-end server for processing. Ciphertext is used extensively throughout the process of information exchange.

This study introduces a simple system for protecting patients' personal information while using RFID technology within the framework of the Internet of Things. The obtained data is kept private and safe by the scheme thanks to the use of secure authentication. The procedure has been shown to successfully mitigate the danger of unauthorized disclosure of sensitive medical information via examination and analysis of its security measures.

### III. METHODOLOGY

Secure user data is a top priority, thus we're using blockchain and AI in private data centers to prevent this problem from occurring. In all, it serves three purposes.

Blockchain—user-guaranteed data sharing based on the blockchain. Using this method, the data owner may decide which users have access to his information and which do not, much like a typical user permissions system. If one person grants access to another user in a blockchain, only the latter will be able to see the data. Second, AI-based secure computing platforms generate smarter security rules, and AI aids in the building of a more trustworthy and safe online environment.

Artificial intelligence will function similarly to the human brain in that it will be responsible for executing reasoning, such as checking whether or not a user has been granted access to shared data.

### IV. RESULT AND DISCUSSION

I'm inputting the patient's medical history and selecting Hospital1 for submission; if you want to submit to both hospitals at once, hold down the CTRL key while selecting the second hospital. Just click the create account button below to get started.

The following page displays the patient's complete information together with the hash code issued by the blockchain, and the final column displays the patient reward income, which will be updated with each access by a hospital user.



Fig 1. Hospital Login.



Fig 2. Displaying patient's information.

### V. CONCLUSION

We propose the SecNet, a new networking paradigm that places more emphasis on secure data storage, sharing, and computing than on communication, in order to leverage AI, block chain, and Quantum Computing to address the issue of data abuse and to equip AI with the aid of block chain for trusted data management in a trust-fewer environments. SecNet uses blockchain technology to guarantee data ownership, while also providing a secure computing platform powered by artificial intelligence and an incentive mechanism based on the blockchain. This allows for the merging of data and the development of more advanced AI, which ultimately leads to increased network security.

In addition, we go through a typical scenario for deploying SecNet in a healthcare setting, and we provide several other methods for making use of SecNet's storage capabilities. In addition, we assess its effectiveness in reducing network exposure to DDoS assaults and evaluate its novel approach to enticing users to share security rules for a better protected network. In our future research, we want to investigate the feasibility of using blockchain to authorize data access requests and to develop robust smart contracts for data exchange and AI- based computing in

SecNet. Furthermore, we will model SecNet and evaluate its efficacy by conducting comprehensive tests on state-of-the-art systems (e.g., integrating IPFS and Ethereum to form a SecNet-like architecture).

## REFERENCES

- [1] Mahammad, Farooq Sunar, et al. "Prediction of Covid-19 Infection Based on Lifestyle Habits Employing Random Forest Algorithm." *Journal of Algebraic Statistics* 13.3 (2022): 40-45.
- [2] [2]Devi, M. Sharmila, et al. "Machine Learning Based Classification and Clustering Analysis of Efficiency of Exercise against Covid-19 Infection." *Journal of Algebraic Statistics* 13.3 (2022): 112-117.
- [3] Bhaskar, P., Mahammad, F. S., Kumar, A. H., Kumar, D. R., Khadar, S. A., Khan, P. M., & Reedy, P. V. S. (2022). Machine Learning Based Predictive Model for Closed Loop Air Filtering System. *Journal of Algebraic Statistics*, 13(3), 609-616.
- [4] Gowthami, V., et al. "Knowledge Based System for Immunity Improvement against Covid-19 Infection." *Journal of Algebraic Statistics* 13.3 (2022): 01-07.
- [5] Mahammad, Farooq Sunar, et al. "Heuristics Approach Based Expert System for Covid-19 Infection Susceptibility." *Journal of Algebraic Statistics* 13.3 (2022): 46-51.
- [6] Reddy, E. Madhusudhana and P. Bhaskar. "Able Machine Learning Method for classifying Disease-Treatment Semantic Relations from Bio-Medical Sentences." vol 5 (2018): 5.
- [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.