Forest Fire Detection using CNN-RF and CNN-XGBOOST Machine Learning Algorithms

Kambala Jagadish
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
B.S.Murthy
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

Abstract: In the digital age, securing data has become increasingly critical due to the exponential growth of cyber threats and data breaches. This project explores a hybrid approach to data security by integrating Blockchain technology and Artificial Intelligence (AI). Blockchain provides a decentralized, immutable ledger that ensures transparency, integrity, and tamper-proof storage of data. On the other hand, AI enhances security by enabling intelligent threat detection, anomaly analysis, and predictive analytics through machine learning algorithms. By combining these two powerful technologies, the proposed system leverages Blockchain for secure data storage and traceability, while AI automates the identification of potential vulnerabilities and malicious activities in real-time. This synergy enhances the overall cybersecurity posture by ensuring not only the safety and privacy of data but also the adaptability of the system to evolving threats. The solution has applications across industries such as healthcare, finance, and supply chain, promoting trust, compliance, and resilience in digital ecosystems.

I. INTRODUCTION

With the development of information technologies, the trend of integrating cyber, physical and social (CPS) systems to a highly uni_ed information society, rather than just a digital internet, is becoming increasing obvious [1]. In such an information society, data is the asset of its owner, and its usage should be under the full control of its owner, although this is not the common case [2], [3].

Given data is undoubtedly the oil of the information society, almost every big company want to collect data as much as possible, for their future competitiveness [4], [5]. An increasing amount of personal data, including location information, web-searching behavior, user calls, user preference, is being silently collected by the built-in sensors inside the products from those big companies, which brings in huge risk on privacy leakage of data owners [6], [7]. Moreover, the usage of those data is out of control

of their owners, since currently there is not a reliable way to record how the data is used and by who, and thus has little methods to trace or punish the violators who abuse those data [8]. That is, lack of ability to effectively manage data makes it very dif_cult for an individual to control the potential risks associated with the collected data [9]. For example, once the data has been collected by a third party (e.g., a big company), the lack of access to this data hinders an individual to understand or manage the risks related to the collected data from him. Meanwhile, the lack of immutable recording for the usage of data increases the risks to abuse them [10]. merge the data scattered across the whole CPS to form real big data, the performance of arti_cial intelligence (AI) will be signi_cantly improved since AI can handle massive amount of data including huge information at the same time, which would bring in great bene_ts (e.g., achieving enhanced security for data) and even makes AI gaining the ability to exceed human capabilities in more areas [11]. According to the research in [12], if given large amount of data in an orders of magnitude more scale, even the simplest AI algorithm currently (e.g., perceptrons from the 1950s) can achieve fanciest performance to beat many state-of-the-art technologies today. The key lies in how to make data sharing trusted and secured [13]. Fortunately, the blockchain technologies may be the promising way to achieve this goal, via consensus mechanisms throughout the network to guarantee data sharing in a tamper-proof way embedded with economic incentives [14], [15]. Thus, AI can be further empowered by blockchain-protected data sharing [16]_[18]. As a result, enhanced AI can provide better performance and security for data.

In this paper, we aim at securing data by combining blockchain and AI together, and design a Secure Networking architecture (termed as SecNet) to signi_cantly improve the security of data sharing, and then the security of the whole network, even the whole CPS.

II.   LITEARTURE SURVEY

1. Hyperconnected network: A decentralized trusted computing and networking paradigm

Abstract:

With the development of the Internet of Things, a complex CPS system has emerged and is becoming a promising information infrastructure. In the CPS system, the loss of control over user data has become a very serious challenge, making it difficult to protect privacy, boost innovation, and guarantee data sovereignty. In this article, we propose HyperNet, a novel decentralized trusted computing and networking paradigm, to meet the challenge of loss of control over data. HyperNet is composed of the intelligent PDC, which is considered as the digital clone of a human individual; the decentralized trusted connection between any entities based on blockchain as well as smart contract; and the UDI platform, enabling secure digital object management and an identifier-driven routing mechanism. HyperNet has the capability of protecting data sovereignty, and has the potential to transform the current communication-based information system to the future data-oriented information society.

2. Lightweight RFID protocol for medical privacy protection in IoT

Abstract:

Traditional medical privacy data are at a serious risk of disclosure, and many related cases have occurred over the years. For example, personal medical privacy data can be easily leaked to insurance companies, which not only compromises the privacy of individuals, but also hinders the healthy development of the medical industry. With the continuous improvement of cloud computing and big data technologies, the Internet of Things technology has been rapidly developed. Radio frequency identification (RFID) is one of the core technologies of the Internet of Things. The application of the RFID system to the medical system can effectively solve this problem of medical privacy. RFID tags in the system can collect useful information and conduct data exchange and processing with a back-end server through the reader. The whole process of information interaction is mainly in the form of ciphertext. In the context of the Internet of Things, the paper presents a lightweight RFID medical privacy protection scheme. The scheme ensures security privacy of the collected data via secure authentication. The security analysis and evaluation of the scheme indicate that the protocol can effectively prevent the risk of medical privacy data being easily leaked.

3. Amber: Decoupling user data from Web applications

Abstract:

User-generated content is becoming increasingly common on the Web, but current web applications isolate their users' data, enabling only restricted sharing and cross-service integration. We believe users should be able to share their data seamlessly between their applications and with other users. To that end, we propose Amber, an architecture that decouples users' data from applications, while providing applications with powerful global queries to find user data. We demonstrate how multi-user applications, such as e-mail, can use these global queries to efficiently collect and monitor relevant data created by other users. Amber puts users in control of which applications they use with their data and with whom it is shared, and enables a new class of applications by removing the artificial partitioning of users' data by application.

4. Enhancing selectivity in big data

Abstract:

Today's companies collect immense amounts of personal data and enable wide access to it within the company. This exposes the data to external hackers and privacy-transgressing employees. This study shows that, for a wide and important class of workloads, only a fraction of the data is needed to approach state-of-the-art accuracy. We propose selective data systems that are designed to pinpoint the data that is valuable for a company's current and evolving workloads. These systems limit data exposure by setting aside the data that is not truly valuable.

III.   PROPOSED METHOD

To overcome from above issue author has describe concept called Private Data Centres (PDC) with Blockchain and AI technique to provide security to user's data. In this technique 3 functions will work which describe below

1) Blockchain: Blockchain-based data sharing withownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data. In this technique users can define access control which means which user has permission to access data and which user cannot access data and Blockchain object will be generate on that access data and allow only those users to access data which has permissions. In Blockchain object user will add/subscribe share data and give permission.

2) Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to constructa more trusted cyberspace. AI work similar to human brain and responsible to execute logic to check whether requesting user has permission to access shared data. If access is available then AI allow Blockchain to display share data otherwise ignore request.

3) Rewards: In this technique all users who is sharing the data will earn rewards point upon any user access his data. trusted value-exchange mechanism for purchasing security service, providinga way for participants to gain economic rewards when giving out their data or service, which promotes thedata sharing and thus achieves better performance of AI.

IV. RESULTS

Deploy code on DJANOGO and start server and run in browser to get below screen

In above screen click on 'New Patient Register Here' link to get below screen

In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile

In above screen one patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1
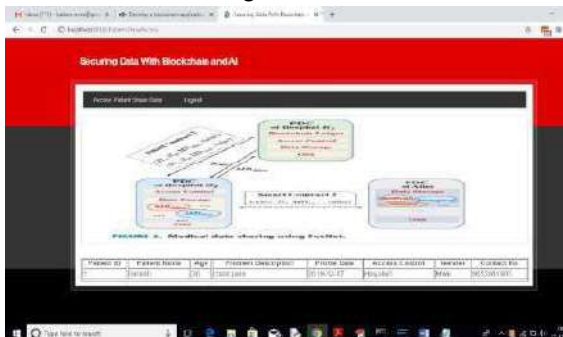

In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen

In above screen click on 'Access Patient Share Data' link to search for patient details

In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen

In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'

In above screen 'Hospital2' is login, after login will get below screen

Now click on 'Access Patient Share Data' link and search for same pain disease

For above query will get below result

In above screen no patient details are showing as Hospital2 not having permission. So block chain allow only those users to access data who has permission. Now logout and login as patient by entering patient id in below screen

After login will get below details for patient 1
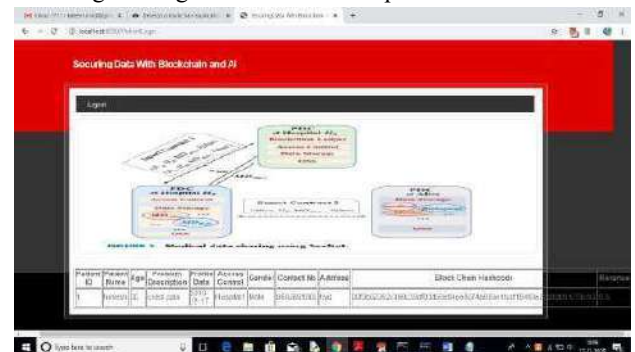
In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

V. CONCLUSION

In order to leverage AI and blockchain to _t the problem of abusing data, as well as empower AI with the help of blockchain for trusted data management in trust-less environment, we propose the SecNet, which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating. SecNet provides data ownership guaranteeing with the help of blockchain technologies, and AI-based secure computing platform as well as blockchain-based incentive mechanism, offering paradigm and incentives for data merging and more powerful AI to finally achieve better network security. Moreover, we discuss the typical use scenario of SecNet in medical care system, and gives alternative ways for employing the storage function of SecNet. Furthermore, we evaluate its improvement on network vulnerability when countering DDoS attacks, and analyze the inventive aspect on encouraging users to share security rules for a more secure network. In future work, we will explore how to leverage blockchain for the access authorization on data requests, and design secure and detailed smart contracts for data sharing and AI-based computing service in SecNet. In addition, we will model SecNet and analyze its performance through extensive experiments based on advanced platforms (e.g., integrating IPFS [27] and Ethereum [28] to form 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. S

[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.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.

[6] 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.

[7] Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study for product traceability,'' IEEE Softw., vol. 34, no. 6, pp. 21_27, Nov./Dec. 2017.

[8] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ``Deep learning based inference of private information using embedded sensors in smart devices'' IEEE Netw. Mag., vol. 32, no. 4, pp. 8_14, Jul./Aug. 2018.

[9] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,'' IEEE Access, vol. 5, pp. 14757_14767, 2017.

[10] D. E. O'Leary, ``Arti_cial intelligence and big data,'' IEEE Intell. Syst., vol. 28, no. 2, pp. 96_99, Mar. 2013.

[11] A. Halevy, P. Norvig, and F. Pereira, ``The unreasonable effectiveness of data,'' IEEE Intell. Syst., vol. 24, no. 2, pp. 8_12, Mar. 2009.

[12] Z. Cai and X. Zheng, ``A private and ef_cient mechanism for data uploading in smart cyber-physical systems,'' IEEE Trans. Netw. Sci. Eng., to be published. doi: 10.1109/TNSE.2018.2830307.

[13] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, ``BlockChain: A distributed solution to automotive security and privacy,'' IEEE Commun. Mag., vol. 55, no. 12, pp. 119_125, Dec. 2017.

[14] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ``A blockchain based privacy-preserving incentive mechanism in crowdsensing applications,'' IEEE Access, vol. 6, pp. 17545_17556, 2018.