BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE BASED ENHANCED SECURITY IN DATA ENGINEERING

Dr. Santosh Kumar Byraboina [1], Ms. Janke. Kalyani [2], Dr. PM Yohan [3]

[1]Associate Professor, Department of MCA,Wesley PG College, Secunderabad.

[2]Assistant professor, Dept of Computer Science, University PG College, Osmania University, Secunderabad.

[3]Professor and Principal, CSI Wesley Institute of Technology And Sciences, Secunderabad.

Abstract

Data is used as input by various artificial intelligence (AI) algorithms to mine important characteristics; however, data on the Internet is distributed and controlled by disparate stakeholders that lack mutual trust, and it is challenging to evaluate or authorize the use of data in complicated cyberspace. Enabling data sharing for actual vast data and true powerful AI in cyberspace is therefore quite difficult. We describe here the Sec-Net architecture, which can facilitate safe data sharing, computation, and storing in the context of the large-scale Internet. The Sec-Net seeks to improve AI with numerous data sources and a more secure cyberspace by merging these three essential components. 1) A safe computing platform based on artificial intelligence (AI) that generates more intelligent security rules, contributing to the creation of a more trustworthy cyberspace; 2) Blockchain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form true big data; 3) Trusted Value: By providing participants with a way to be paid financially for providing their services or data, exchange mechanisms for security services promote data sharing and enhance AI performance. In addition to going over Sec-Net's typical use case and different deployment choices, we also analyze its efficacy in terms of both financial gain and network security.

Index Terms:- block chain,sha256,, artificial intelligence ,Trusted Value. **Sec-Net**

I Introduction

The tendency of combining cyber, physical, and social (CPS) systems into a highly integrated information society, rather than merely a digital Internet, is becoming more and more visible with the advancement of information technologies. Data is an asset of its owner in such an information society, and their use should be completely within their control, albeit this is not always the case. Given that data is unquestionably the lifeblood of the information age, practically every major corporation wants to gather as much data as they can to stay competitive in the future. A growing amount of personal information, such as location data, web search history, and user calls, The built-in sensors inside the goods from such large corporations secretly record user preferences, which poses a serious risk to the data owners' privacy. Furthermore, the owners of that data have no influence over how they are used because there is currently no reliable way to keep track of who is using them and how, and there are few ways to find or punish those violators [8]. In other words, it is very difficult for a person to control any potential hazards related with the obtained data when they lack the ability to manage data efficiently. For instance, once the data has been gathered by a third party (such as a large firm), the inability to access this data can be detrimental.. Meanwhile, the lack of immutable recording for the usage of data increases the risks to abuse them . If there is an efficient and trusted way to collect and merge the data scattered across the whole CPS to form real big data, the performance of artificial intelligence (AI) will be significantly improved since AI can handle massive amount of data including huge information at the same time, which 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 .

2 Literature survey

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

Abstract:
A complicated CPS system has arisen with the growth of the Internet of Things and is developing into a viable information infrastructure. It has become increasingly challenging to safeguard data sovereignty, promote innovation, and preserve privacy in the CPS system due to the loss of control over user data. To address the issue of data loss of control, we suggest Hyper-Net in this essay, a revolutionary decentralised trustworthy computing and networking paradigm. The

intelligent PDC, which is regarded as a digital copy of a human person, the decentralised trusted connection between any entities based on blockchain and smart contracts, and the UDI platform, which supports secure digital object management and an identifier-driven routing mechanism, are the components that make up Hyper-Net. Hyper-Net is equipped to Hyper-Net 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.

2.2Lightweight 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 exchange of information takes place mostly through cypher text. The study provides a minimal RFID medical privacy protection method within the Internet of Things. Through secure authentication, the system guarantees the confidentiality and privacy of the obtained data. According to the security analysis and scheme evaluation, the protocol may successfully reduce the risk of medical privacy data being easily disclosed.

2.3Amber: 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.

2.4Enhancing selectivity in big data

Abstract:

Large-scale internal access to personal data is made possible by the massive volumes of data that modern businesses collect. This makes the data accessible to outside hackers and workers who violate privacy. This study demonstrates that only a small portion of the data is required to achieve state-of-the-art accuracy for a large and significant class of workloads. We suggest selective data systems that are made to focus on the information that is important for a business's ongoing and changing demands. By excluding the data that isn't actually valuable, these technologies reduce the amount of data that is exposed.

3. Methodology

3.1 Implementation Study

In the digital world, everything is dependent on data, and all artificial intelligence algorithms learn from past data only. For instance, in online shopping applications, user review data is crucial for assisting new users in deciding whether to buy a product or not. Other examples include health care, where knowing the best hospitals or educational institutions is important. Not all cyber data can be made public, such as patient health data, which includes contact information and information about the patient's ailment. If such data is made public, there is no protection for the patient data.Now a days all service providers such as online social networks or cloud storage will store some type of users data and they can sale that data to other organization for their own benefits and user has no control on his data as that data is saved on third party servers.

3.2 proposed methodology

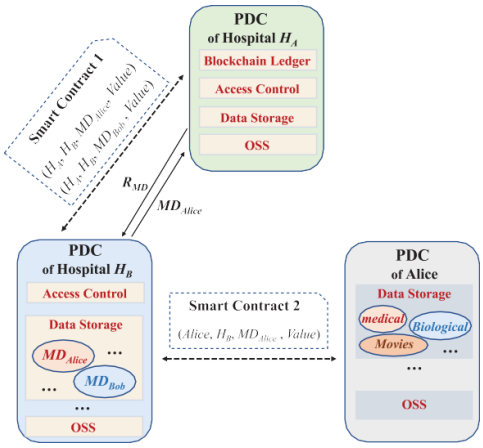
To overcome from above issue author has describe concept called Private Data Centres (PDC) with Block chain and AI technique to provide security to user's data. In this technique 3 functions will work which describe below

Block chain: Trusted data sharing in a large-scale setting is made possible by block chain-based data sharing with ownership guarantees, which creates actual big data. In this method, users can specify access control, i.e., which users can access data and which users cannot, and a block chain object will be generated on the data that can be accessed, allowing only those users to do so. The user will add, subscribe, share, and grant authorization for a block chain object.

Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to construct a more trusted cyberspace.

Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to construct a 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.

- **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, providing a way for participants to gain economic rewards when giving out their data or service, which promotes the data sharing and thus achieves better performance of AI



.

Fig 1: - proposed model

Patients: Patients first create his profile with all disease details and then select desired hospital with whom he wishes to share/subscribe data. While creating profile application will create

Blockchain object with allowable permission and it will allow only those hospitals to access data.

Patient Login: Patient can login to application with his profile id and check total rewards he earned from sharing data.

Hospital: Hospital1 and Hospital2 are using in this application as two organizations with whom patient can share data. At a time any hospital can login to application and then enter search string as disease name.

AI algorithm will take input disease string and then perform search operation on all patients to get similar disease patients and then check whether this hospital has permission to access that patient data or not, if hospital has access permission then it will display those patients records to that hospital.

4. Results and Evolution Metrics

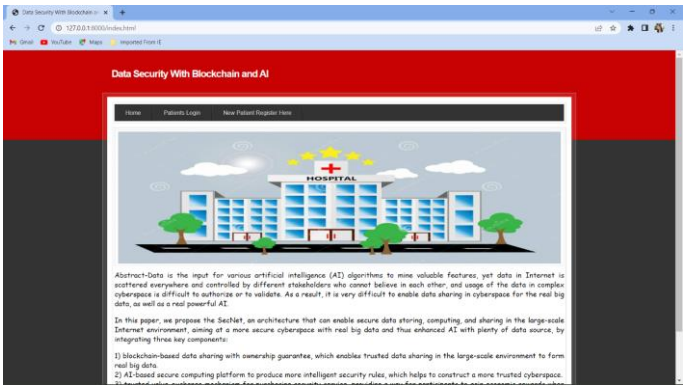


Fig 2:_ In above screen click on 'New Patient Register Here' link to get below screen

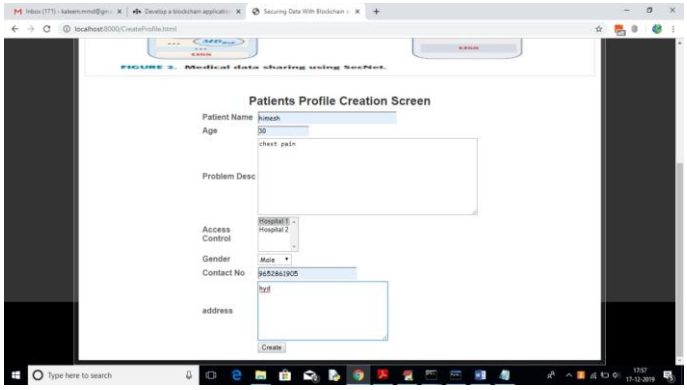


Fig 3:- In above screen I am adding patient disease details and selecting ‘Hospital1’ to share my data and if you want to share with two hospitals then hold ‘CTRL’ key and select both hospitals to give permission. Now press ‘Create’ button to create profile

Fig 4:- 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

Fig5:- 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

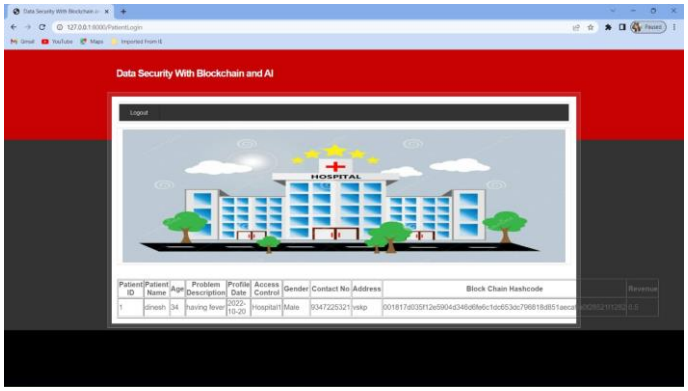


Fig 6:- In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as Hospital2.

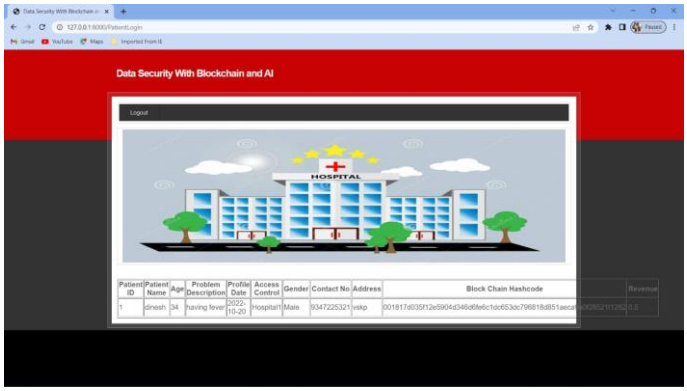


Fig 7:- In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

5. Conclusion

To address the issue of data abuse and enable AI with the help of blockchain for trusted data management in a trust-less environment, we propose The Sec-net, a new networking paradigm that focuses on secure data storing, sharing, and computing instead of communication. Sec-net provides data ownership ensuring through blockchain technologies, an AI-based secure computing platform, and a blockchain-based reward system. Additionally, it offers a paradigm and incentives for data fusion and stronger AI, which will ultimately enhance network security. We also go over sec-net's typical use case in the healthcare sector and offer some other ways to make use of its storing capabilities. Furthermore, We Evaluate Its Improvement On Network Vulnerability When Countering Ddos Attacks, And Analyse The Inventive Aspect On Encouraging Users To Share Security Rules For A More Secure Network.

.

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 Net., vol. 32, no. 1, pp. 112117, 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. 16561665, 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. 16.

[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. 3442, 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 Compute., vol. 2, no. 4, pp. 4453, 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 Common. Mag., vol. 56, no. 9, pp. 5561, Sep. 2018.

[8] Q. Lu and X. Xu, ``Adaptable blockchain-based systems: A case study for product traceability," IEEE Soft., vol. 34, no. 6, pp. 2127, Nov./Dec. 2017.

[9] 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 Net. Mag., vol. 32, no. 4, pp. 814, Jul./Aug. 2018.