



SECURING DATA WITH BLOCK CHAIN AND ARTIFICIAL INTELLIGENCE

S. Ramya Assistant professor , I.T DEPT, Vijaya College, Vijawada, Andharapradesh

Email:- ramyaswarna6@gmail.com

CH.Lakshmi Sowjanya , V.Ashmitha , S.Lakshmi Hari Chandhana , V.Suharshitha ,Betch

Student of I.T DEPT, **Vijaya College**, Vijawada, Andharapradesh

Email:- saripalisrimukhesh@gmail.com

Abstract

Data is the input for various artificial intelligence (AI) algorithms to mine valuable features, yet data in Internet is scattered everywhere and controlled by different stakeholders who cannot believe in each other, and usage of the data in complex cyberspace is difficult to authorize or to validate. As a result, it is very difficult to enable data sharing in cyberspace for the real big data, as well as a real powerful AI. In this paper, we propose the **Sec-Net**, an architecture that can enable secure data storing, computing, and sharing in the large-scale Internet environment, aiming at a more secure cyberspace with real big data and thus enhanced AI with plenty of data source, by integrating three key components:

- 1) Blockchain- Based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data;
- 2) AI - Based secure computing platform to produce more intelligent security rules, which helps to construct a more trusted cyberspace;
- 3) 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. Moreover, we discuss the typical use scenario of Sec-Net as well as its potentially alternative way to deploy, as well as analyze its effectiveness from the aspect of network security and economic revenue.

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

I Introduction

With the development of information technologies, the trend of integrating cyber, physical and social (CPS) systems to a highly unified information society, rather than just a digital Internet, is becoming increasing obvious . 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 . 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 . An increasing amount of personal data, including location information, web-searching behaviour, 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 . 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 difficult for an individual to control the potential risks associated with the collected data . 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 . 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:

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 Hyper-Net, a novel decentralized trusted computing and networking paradigm, to meet the challenge of loss of control over data. Hyper-Net 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. 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 whole process of information interaction is mainly in the form of cipher text. 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.

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.



2.4 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.

3. Implementation Study

In cyber world everything is dependent on data and all Artificial Intelligence algorithms discover knowledge from past data only, for example in online shopping application users review data is very important for new comers to take decision on which product to purchase or not to purchase, we can take many examples like health care to know good hospitals or education institutions etc. Not all cyber data can be made publicly available such as Patient Health Data which contains patient disease details and contact information and if such data available publicly then there is no security for that 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.

3.1 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: Block chain-based data sharing with ownership 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 Block chain object will be generate on that access data and allow only those users to access data which has permissions. In Block chain object user will add/subscribe share data and give permission.

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

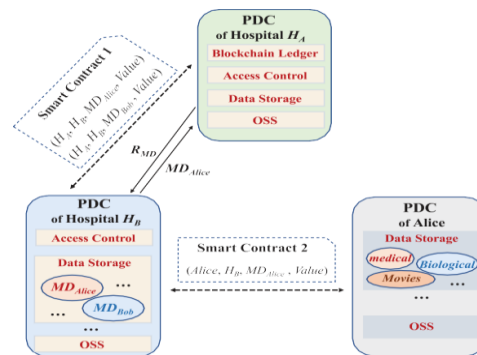


Fig 1: - proposed model

4 Methodology

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.

5 Results and Evolution Metrics

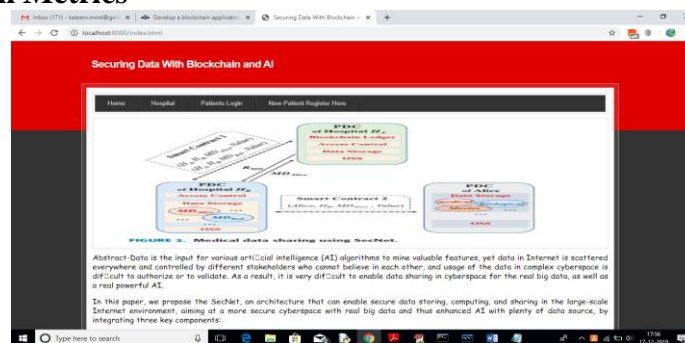


Fig 2: _ In above screen click on 'New Patient Register Here' link to get below screen

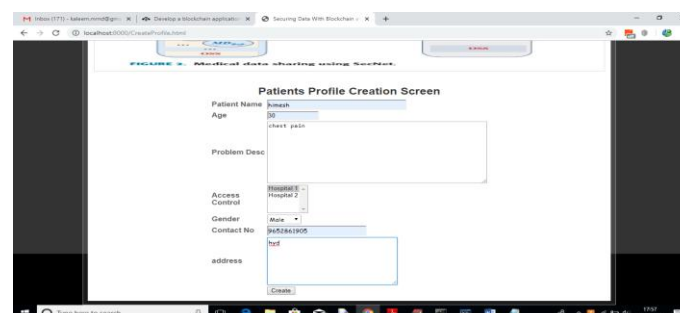


Fig 3:- In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile

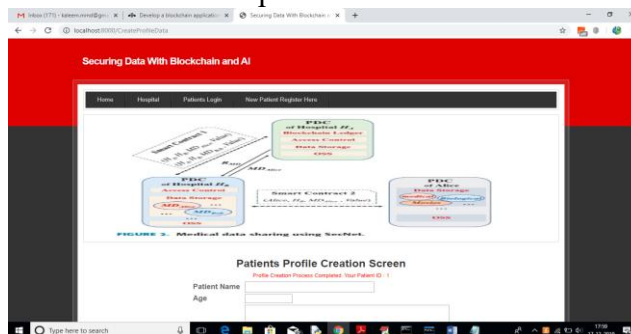


Fig 4:- In above screen one patient is created with patient ID 1 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1

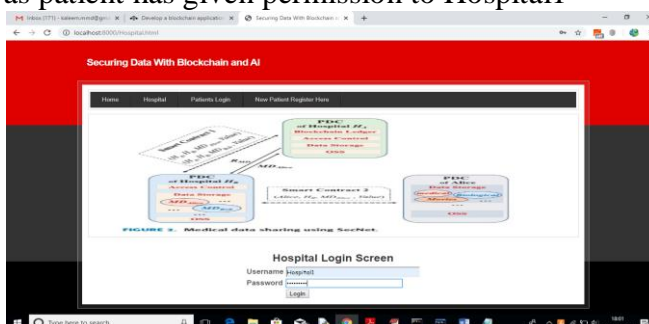


Fig5:- In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen

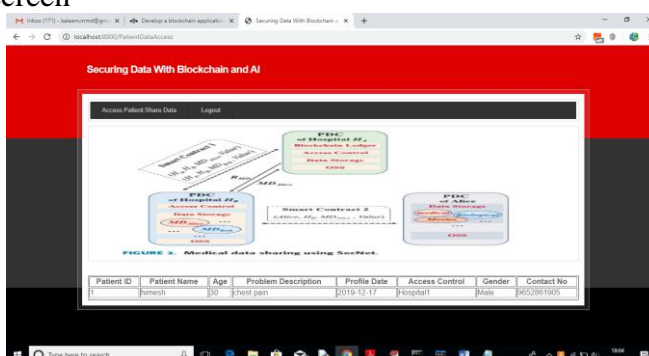


Fig 6:- In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as Hospital2.

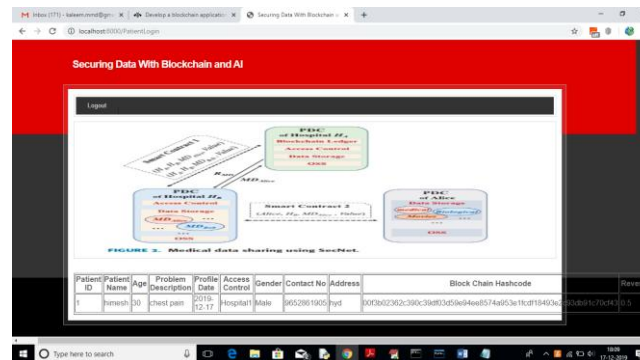


Fig 7:- In above screen we can see patient all details and hash code generated by block chain and in last column we can see patient reward revenue as 0.5 and it will get update upon every access from hospital user.

5 Conclusion

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 Sec-net, Which Is A New Networking Paradigm Focusing On Secure Data Storing, Sharing And Computing Instead Of Communicating. Sec-net Provides Data Ownership Guaranteeing With The Help Of Blockchain Tech- Neologies, 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 Nally Achieve Better Network Security. Moreover, We Discuss The Typical Use Scenario Of Sec-net 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 Analyse The Inventive Aspect On Encouraging Users To Share Security Rules For A More Secure Network.

6 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. [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.