PREVENTION OF DATA HACKING WITH BLOCKCHAIN

Mrs.ROJARAMANI
Assistant Professor
Department of Computer Science and Engineering
Email: roja.adapa@tkrec.ac.in
TEEGALA KRISHNA REDDY ENGINEERING COLLEGE,
HYDERABAD

PEDDI VENKATARAMANA, PAVITHRA, SATHVIK REDDY
Under Graduate Students
Department of Computer Science and Engineering
Email: peddivenkataramana78@gmail.com, pavibathula1@gmail.com, sathvik733@gmail.com
TEEGALA KRISHNA REDDY ENGINEERING COLLEGE, HYDERABAD – 500097

ABSTRACT: Data is the input for various 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. In this 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 with plenty of data source, by integrating key component: Block chain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data.

I. INTRODUCTION

All these ideas and solutions above propose to protect data security, by designing a new service paradigm supporting the decoupling of data and application, or by designing a specific blockchain to meet demands of certain applications, or by integrating as a functional component to analyze data security. However, none of them treats the problem of data security from the view of architecture. To fill this gap, SecNet tries to construct a common and general networking architecture by the power of blockchain at a large scale, which can support dynamic update of all these functional component separately at any time as needed, to efficiently and effectively improve the data security for all applications .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.

II. LITERATURE SURVEY

With the development of the Internet of Things, a complex CPS system has emerged and 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.

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.

III. EXISTING SYSTEM

In existing private data centers (PDC) is done manually without user permissions and security. Data is given to third party person. All service provider such as online social network or cloud storage will store some type of user 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 server.

DISADVANTAGE:

Low level security (password , fingerprint , facial recognition ,OTP & etc) - In online banking , the user can't connect directly to the bank server for his requirements like money transactions .There will be the third party control,where they will check the user details and gives access to the bank server, in this way the third party is involved in between user and the bank for their own benefits they can sell the user data to other organizations .

IV. PROPOSED SYSTEM

To overcome this issue we proposed private data centre with block chain to provide security to user's data. We can share data with high security without involving other persons that is third-party user. By block chain, we designed a secure networking architecture (Sec Net) to significantly improve the security of data sharing and then the security of whole network.

MERITS OF PROPOSED SYSTEM

- Full security
- Transparency
- Immutability
- Without dependency on third party

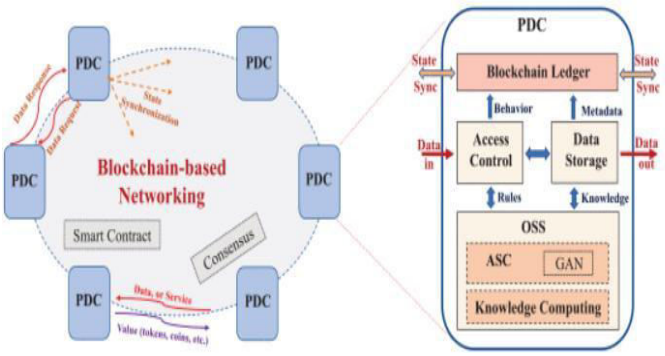
V. ALGORITHM OF THE PROJECT

SHA-256

The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long. In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size.

5.1 SYSTEM ARCHITECTURE

Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. The block diagram is typically used for a higher level, less detailed description aimed more at understanding the overall concepts and less at understanding the details of implementation.



VI. SYSTEM IMPLEMENTATION

MODULES

This project consists of three modules:

- **Customer** : Customer first create his profile with all details and then select desired company 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 companies to access data.

  Customer Login: Customer can login to application with his profile id.

- **Admin:** The admin will check the authorization of the company and customer for providing the demanded information.

- **Company** :

  Company 1 and Company 2 are using in this application as two Organizations with whom customer can share data. At a time any company can login to application.

VII.CONCLUSION

In order to average Blockchain to fit the problems of abusing data and with the help of blockchain for trusted data management SecNet which is a new networking paradigm focusing on secure data storing, sharing and computing instead of communicating SecNet provide ownership guaranteeing with the help of block chain for better network security.

VIII.FUTURE ENHANCEMENT

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 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).

BIBLIOGRAPHY

[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,

[4] 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.

[5] 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.

[6] 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.

[7] C. Perera, R. Ranjan, and L. Wang, ‘‘End-to-end privacy for open big data markets,’’ IEEE Cloud Computes., vol. 2, no. 4, pp. 44–53, Apr. 2015.

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