SECURING DATA USING BLOCKCHAIN AND AI

[1]G. BHARATHI,[2] N.SAITEJA, [3]R. SANDEEP, [4]V. ABHILASH, [5]Y. SAI BHARGHAV REDDY

[1](Assistant Professor), CSE, J.B. Institute Of Engineering & Technology

[2345]B.Tech Scholar, CSE, J.B. Institute Of Engineering & Technology

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 SecNet, 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:

Block chain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-scale environment to form real big data.AI-based secure computing platform to produce more intelligent security rules, which helps to construct a more trusted cyberspace. 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.

1. INTRODUCTION

1.1 MOTIVATION

Securing data using blockchain and AI is a compelling project with a range of motivations, given the potential benefits that these technologies can offer. 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 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. 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.

The key lies in how to make data sharing trusted and secured. 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. Thus, AI can be further empowered by blockchain-protected data sharing . 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 significantly improve the security of data sharing, and then the security of the whole network, even the whole CPS. In SecNet, to protect data, one of the biggest challenges is where and how to store data, because users have to give their data to service providers if they want to use certain services or applications.This is caused by the inherent coupling of user data and application in current service mechanisms, which significantly hinders the development of data protection and application innovation.

1.2PROBLEM DEFINITION

In today's digital age, organizations face the challenge of securing vast amounts of data while ensuring its integrity, privacy, and availability. Traditional data storage and management methods often fall short due to vulnerabilities such as centralized control, data breaches, and lack of transparency. Moreover, the ever-evolving landscape of cyber threats requires adaptive and intelligent security measures.In SecNet, to protect data, one of the biggest challenges is where and how to store data, because users have to give their data to service providers if they want to use certain services or applications.

The combination of blockchain and AI offers a novel approach to these challenges, providing decentralized, tamper-resistant data storage, and intelligent data management.Embedding PDC into SecNet would allow users to monitor and reason about what and why their data is used as well as by who, meaning the users can truly control every operation on their own data and achieve fine-grained management on access behaviors for data. Actually, besides PDC, other choices can also be applied for the data storing in SecNet according to certain requirements (see Section V). The trust-less relationship between different data stakeholders significantly thwarts the data sharing in the whole Internet, thus the data used for AI training or analyzing is limited in amount as well as partial in variety.

The challenge is to develop a robust system that leverages blockchain and AI to provide a secure, scalable, and efficient data management solution while overcoming the aforementioned issues and meeting the needs of various industries such as finance, healthcare, and logistics. The system must strike a balance between data privacy, security, and accessibility, providing a clear audit trail and enabling intelligent data-driven decision-making.

1.3 OBJECTIVE

The primary objective of the project is to design and implement a robust, secure, and scalable data management system that leverages the combined strengths of blockchain and AI technologies. This system aims to address the challenges of data security, integrity, privacy, and availability in various industries, including finance, healthcare, logistics, and more. Specifically, the project seeks to achieve the following:

- Utilize blockchain's decentralized and tamper-resistant ledger to secure data against unauthorized access, breaches, and alterations.
- Ensure data integrity through blockchain's immutability, providing a transparent and auditable record of data transactions and changes.
- Implement privacy-preserving techniques using AI to manage and process data without compromising sensitive information.

- Develop solutions that address blockchain's scalability challenges and optimize data processing and storage for real-time applications.
- Leverage blockchain's smart contract capabilities, enhanced by AI, to automate data management processes and enforce data governance policies.
- Facilitate seamless integration between different blockchain networks and AI frameworks to ensure smooth data sharing and management across platforms.
- Foster innovation by exploring new applications and opportunities in data management through the combination of blockchain and AI.
- Ensure the system adheres to relevant data protection laws and industry regulations across different jurisdictions.
- Establish mechanisms for verifying the authenticity and provenance of data, as well as the trustworthiness of AI models and smart contracts.
- Design a flexible system that can adapt to emerging technologies and evolving regulatory landscapes.

By achieving these objectives, the project aims to provide organizations with a comprehensive and secure data management solution that supports intelligent decision-making, enhances trust and reputation, and delivers a competitive advantage in the digital era.

2.LITERATURE SURVEY

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

AUTHOR:H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing,

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.

2.2.Lightweight RFID protocol for medical privacy protection in IoT

Author:K. Fan, W. Jiang, H. Li, and Y. Yang, ‘

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 p 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.

2.3.Amber: Decoupling user data from Web applications

AUTHOR:T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, and N. Zeldovich, ‘

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

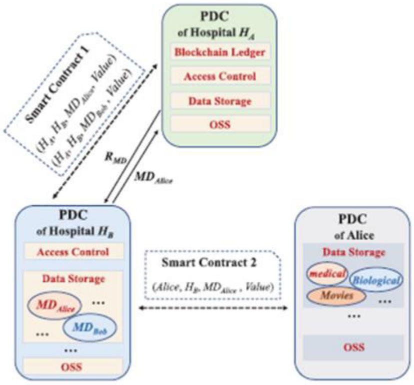
AUTHOR:M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang, and S. Sen

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.

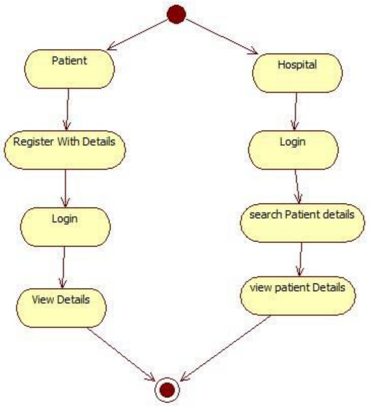
3.SYSTEM DESIGNS

3.1 SYSTEM ARCHITECTURE



ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

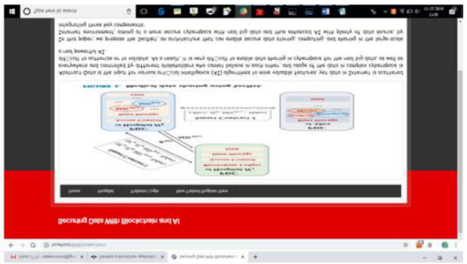


4. OUTPUT SCREENSHOTS

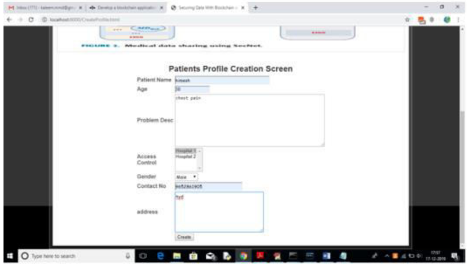
First create database in MYSQL by copying content from 'DB.txt' file and paste in MYSQL.

In settings file change port no from 3308 to 3306 and in 'views.py' file also change port no to 3306

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

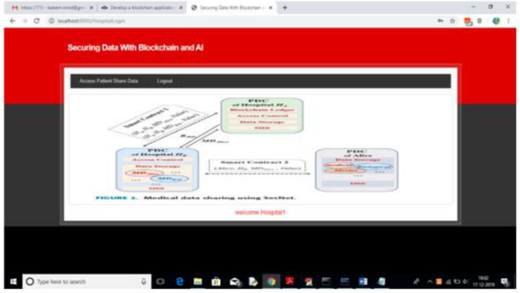


In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile

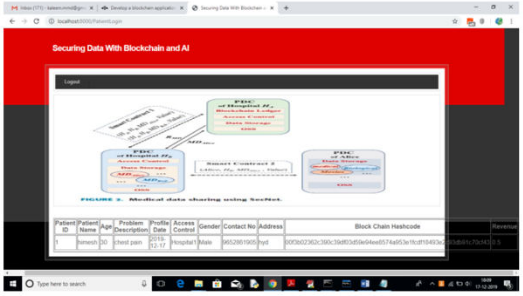

Patients Profile Creation Screen

Patient Name: himesh
Age: 30
Problem Desc: chest pain
Access Control: Hospital 1, Hospital 2
Gender: Male
Contact No: 9652861905
address: hyd

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


Securing Data With Blockchain and AI
Access Patient Share Data
Logout
FIGURE 2. Medical data sharing using SecNet.

welcome Hospital1


Securing Data With Blockchain and AI
Logout
FIGURE 2. Medical data sharing using SecNet.

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No	Address	Block Chain Hashcode	Revenue
1	himesh	30	chest pain	2019-12-17	Hospital1	Male	9652861905	hyd	00f3b02362c390c39df03d59e94ee8574a953e1fcdf18493e2[illegible]db61c70cf43	0.5

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 SecNet, which is a new network- ing paradigm focusing on secure data storing, sharing and computing instead of communicating. SecNet provides data ownership guaranteeing with the help of blockchain tech- nologies, 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 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 exten- sive experiments based on advanced platforms (e.g., inte- grating IPFS [27] and Ethereum [28] to form a SecNet-like architecture).

6. FUTURE SCOPE

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).The integration of blockchain and AI presents a promising future for securing data across various industries. Blockchain's immutable ledger ensures data integrity and provenance, providing a tamper-proof record of transactions and data exchanges. AI, on the other hand, can analyze blockchain data to detect patterns and anomalies, enhancing security measures and identifying potential threats. This combination enables privacy-preserving computation, such as federated learning, allowing AI models to train on decentralized data without compromising privacy. In identity management, blockchain offers a secure and decentralized approach, while AI provides advanced detection of unusual patterns. Smart contracts on blockchain automate data handling according to predefined rules, and AI can optimize these contracts by detecting inefficiencies. In healthcare, finance, and supply chain, the synergy of blockchain and AI enhances security, transparency, and efficiency. As these technologies evolve, innovative methods for securing data and preserving privacy across various domains will continue to emerge.

7. 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. Sen, ‘‘Enhancing selectivity in big data,’’ IEEE Security Privacy, vol. 16, no. 1, pp. 34–42, 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 Comput., vol. 2, no. 4, pp. 44–53, 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 Commun. Mag., vol. 56, no. 9, pp. 55–61, Sep. 2018.

[8] 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.

[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 Netw. Mag., vol. 32, no. 4, pp. 8–14, Jul./Aug. 2018.

[10] 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.