SECURING DATA WITH BLOCK CHAIN AND AI TECHNIQUES

BADITA BHARGAVI, M.TECH(CSE), Department of Computer Science & Engineering,MVR COLLEGE OF ENGINEERING AND TECHNOLOGY, Beside Hanuman temple, NH9, paritala, Ibrahimpatnam, Andhra Pradesh 521180.

Dr.D.SRINIVAS, Assoc. Professor, Department of Computer Science & Engineering, MVR COLLEGE OF ENGINEERING AND TECHNOLOGY, Beside Hanuman temple, NH9, paritala, Ibrahimpatnam, Andhra Pradesh 521180.

Abstract: 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:

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 SecNet as well as its potentially alternative way to deploy, as well as analyze its effectiveness from the aspect of network security and economic revenue.

INTRODUCTION

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 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 user's 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.

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

1.1 Blockchain: Blockchain-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 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.

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

1.3 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, providing 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.

PROBLEM STATEMENT

- In existing system data protection mechanisms such as encryption was failed in securing the data from the attacker.
- It does not verify whether the user was authorized or not.

PROPOSED SYSTEM

- The proposed system enables Private Data Centres (PDC) with Blockchain and AI technique to provide security to user’s data.
- Blockchain-based data sharing with ownership guarantee, which enables trusted data sharing and generates hash code(unique).

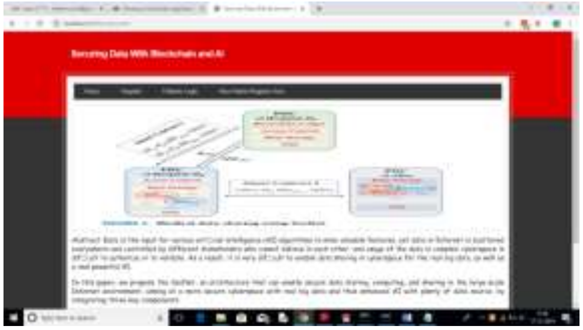
MODULE DESCRIPTION

- **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.

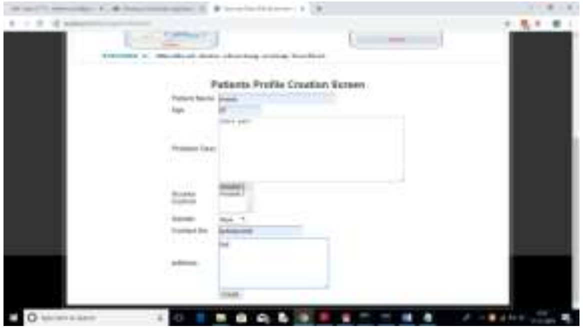
- **Patient Login:** Patient can login to application with his profile id and check total rewards he earned from sharing data.
- **Hospital:** Hospital1 and Hospital2 are using in this application as two organizations with whom patient can share data. At a time, any hospital can login to application 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.

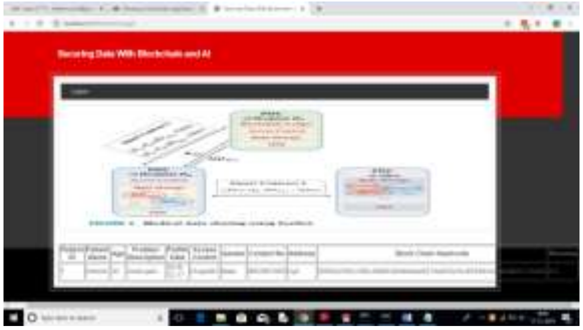
SAMPLE RESULTS



Securing Data With Blockchain and AI



Patients Profile Creation Screen



Securing Data With Blockchain and AI

CONCLUSION & FUTURE WORK

In order to leverage AI and blockchain to fit 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 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. 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.

REFERENCES:

[1] 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, 2019.

[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), WarthWeiningen, 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-toend 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] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, ‘‘Hyper connected network: A decentralized trusted computing and networking paradigm,’’ IEEE Net w., vol. 32, no. 1, pp. 112–117, Jan./Feb. 2018.