Securing Data With Black Chain Technology & AI

1. Dr.I.Satyanarayana,Principal, Sri Indu Institute of Engineering&Technology(SIIET), Sheriguda, Ibrahimpatnam,Hydarabad,
2. D. Nagaraju,Assistant Professor,CSE,SIIET, Sheriguda , Ibrahimpatnam, Hydarabad, emailid:nagarajuindia786@gmail.com
3.SaiVamshi,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
4.Prudhvi,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
5.Nithin,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad
6.J Nagender,Student,CSE,SIIET,Sheriguda,Ibrahimpatnam,Hydarabad

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 dif_cult 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: 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.

Key words: AI, secnet, cyberspace, gain.

I INTRODUCTION

Data and its security have been paramount since the day human beings started accumulating it. Since the earliest stone age era, humans have evolved to process the information around us by various sensory inputs received by different sensory organs. This has led to the development of various arts such as paintings, music,

textures, etc. This thirst for the unknown has made us go into space and advance a significant amount in technology over the years. All of this data created needs to be stored somewhere where it cannot be modified or destroyed, as these are valuable lessons learned throughout the lifetime of an individual or a group which can help the species to grow forward. This has led to the humans collecting and storing a lot of data on various different topics and was accelerated due to the invention of the printing press at which allowed the information to take the form of books that could retain it for a very long time. Another revolution in the storage, retrieval, and access of data happened when the internet was conceived. Electronic storage was already invented by then but the internet added another element to this as the internet allowed the various computers and computing devices all over the world to connect to each other and share information. This was designed to facilitate the exchange of information between the researchers over a large distance to eliminate the need to be physically present at the location to utilize the resources. Due to its initial success, the internet was opened to the public and various different services that used the internet as the backbone started flourishing. The internet started growing exponentially with a lot more users and machines being connected every day. People started using the platform more and more and this led to an increased number of users interacting online. With social media and educational portals, the internet grew to astronomical sizes and the data being produced every day grew to a massive size. With the growth of data and the users online, it created a nourishing environment for people to learn and share valuable skills and information all over the world. The major drawback of open access to everyone on the internet was that there are also some individuals with malicious intent that can ruin the experience of another person purely for personal gain. A lot of users on the internet have valuable and sensitive personal information that is stored in the databases and various organizations to have their internal data that is confidentially stored electronically. This increases the likelihood of an attacker gaining access to this information that would lead to compromised security as well as a huge loss for the organization. This is problematic as there are no alternatives for storage and the convenience offered by the database. Therefore, there is an utmost need to provide a mechanism for controlling the access to the sensitive data through which only the trusted employees and other members of the organization can access the data, based on their hierarchy. This brings forth the blockchain paradigm, being proposed by a group of scientists in the late 1990s the technique was initially developed for use in a

digital notary as it is an excellent choice for tamper-proofing a document. The paradigm was largely unused until it was utilized for the creation of the world's first cryptocurrency. Due to its strong tamper-proof and distributed nature, it is an apt choice for a cryptocurrency. The blockchain is one of the most secure applications and is capable of providing very high security to the data stored and can, therefore, be utilized in an application to safeguard the data and provide an efficient as well as an effective access control mechanism for the sensitive data of an organization.

2. RELATED STUDY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows. S. Yu states that due to rapid pace of technology and the introduction of Internet of Things or IoT, there has been a swift increase in the number of intelligent devices being connected to the internet. These devices are capable of generating a large amount of data due to the fact that it is connected and is interacting with the internet. A large number of devices generate equally large amount of data which cannot be processed efficiently. Therefore, the authors propose an effective technique based on blockchain that can provide a low-cost alternative to create economic value for the IoT data generated. A major drawback of this methodology is that it has the potential to be misused by uploading large amounts of malicious data. R. Wang elaborates on the foundation of network security construction which is the PKI or The Public Key Infrastructure. The researchers also commented on the reliability and the robust security offered by the blockchain platform. Therefore, the authors amalgamated both the methodologies to strengthen the Public Key Infrastructure by a permissioned blockchain that converts the PKI into a privacy-aware PKI. This is crucial as the implementation of a permissioned blockchain also improves the efficiency of the configuration and certificate application. The major drawback is that this technique has been a very specialized approach towards the blockchain paradigm. C. Ehmke explains that the innovative paradigm of Blockchain has been popular and has seen extensive usage recently. The blockchain was utilized for financial applications and that is how it gained immense popularity and limelight. The blockchain was readily picked up by a plethora of researchers and implemented in various different fields, which has greatly helped in bringing increased security to numerous applications. Due to the fact that the blockchain paradigm requires a user of the blockchain to download the whole chain to gain an overview. To ameliorate this effect, the

authors have implemented a scalable and lightweight blockchain protocol. R. Wang introduces the video surveillance system as an irreplaceable tool that can be used to efficiently manage and survey big cities. When a video surveillance system is installed it can easily transmit environment information remotely, this is highly useful as the person does not need to travel long distances and physically be present in the location for the management. Due to a large-scale increase in the monitoring standards with the inclusion of IoT and realtime monitoring, it is susceptible to attacks. Therefore, the authors developed a system for video surveillance based on permissioned blockchains and Convolutional Neural Networks for a seamless and secure system. A Major drawback in the system is that large scale testing of the System has not been performed and will be done in the upcoming researches. J. Lou states that there has been a lack of a key management feature in the Named Data Networking, which is utilized to name each and every object by the producer and also digitally sign it. There are some disadvantages of the conventional approach such as lack of trust between the sites as well as the high chances of failure observed in the centralized architecture if the main node fails. Therefore, the authors in this paper propose an efficient key management scheme based on blockchain for the Named Data Networking paradigm. The blockchain increases the trust between the sites as well as the decentralized architecture is highly useful in overcoming failure. The drawback of the proposed scheme is that it has not been evaluated extensively for its feasibility in reducing the NDN cache pollution. S. Wang explains that there has been a very fast development of cryptocurrency in recent years, which has led to detailed scrutiny of the paradigm. This has uncovered a lot of irregularities in the paradigm such as the Smart Contracts that have been the cause of “The DOA Attack” which has resulted in a huge loss. Therefore, the authors have presented a comprehensive and systematic review of the smart contracts in the blockchain paradigm. The authors have presented a six-layer architecture for smart contracts for increasing the security of the system. The authors have not implemented a formal verification which can provide confidence. Y. Xu introduces the concept of decentralized storage that is based on the blockchain framework. The blockchain is one of the most innovative concepts that can be used to design a highly secure decentralized framework. The authors have proposed section blockchain protocol, which aims to eliminate the storage problem that is encountered in certain devices. The proposed methodology is highly resilient to failure due to the decentralized architecture, as

well as, it has the ability to withstand heavy loads and optimization gracefully due to the implementation of the Blockchain paradigm.

3 METHODOLOGY

Recent increases in security breaches and digital surveillance highlight the need for improved privacy and security, particularly over users' personal data. Advances in cybersecurity and new legislation promise to improve data protection. Blockchain and distributed ledger technologies provide novel opportunities for protecting user data through decentralized identity and other privacy mechanisms. These systems can allow users greater sovereignty through tools that enable them to own and control their own data. Artificial intelligence provides further possibilities for enhancing system and user security, enriching data sets, and supporting improved analytical models.

4 RESULTS EXPLANATION

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. 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) Blockchain: Blockchain-based data sharing withownership 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.
2) Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to constructa 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.

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, providinga way for participants to gain economic rewards when giving out their data or service, which promotes thedata sharing and thus achieves better performance of AI.

Fig.4.1. Home page.

Fig.4.2. Registation page.

Fig.4.3. Hosptial home page.

Fig.4.4. Hosptial 2 module diaply.

Fig.4.5. OUTPUT results.

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.

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 networking 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 tonally achieves 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.

REFERANCES

[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.