BLOCK CHAIN AND AI FOR DATA SECURITY

K. Raj Kiran[1], G. Tanuja[2], N. Suvarna Kumari [3], B. Priyanka [4] ,Sk. Riyaz [5]
[1] Asst. Professor, Krishna Chaitanya Institute of Technology & Sciences , Markapur, A.P, India
[2,3,4,5] Scholar, Krishna Chaitanya Institute of Technology & Sciences , Markapur, India

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) block chain-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 analyse its effectiveness from the aspect of network security and economic revenue.

Keywords: Data security, Data systems, Artificial intelligence, Cyberspace.

[1] 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 [1]. 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 [2], [3]. 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 [4], [5]. 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

[6], [7]. 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 [9].

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 [10]. 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 [11].

According to the research in [12], if given large amount of data in an orders of magnitude more scale, even the simplest AI algorithm currently (e.g., perceptrons from the 1950s) can achieve fanciest performance to beat many state-of-the-art technologies today. The key lies in how to make data sharing trusted and secured [13]. Fortunately, the block chain 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 [14], [15]. Thus, AI can be further empowered by blockchain-protected data sharing [16]–[18]. 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 [1], [3]. 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. Inspired by the concept of Personal Data Store (PDS) from open PDS [5] and the Private Data Center (PDC) from Hyper Net [1], SecNet finally inherits and adopts PDC instead of PDS, as PDC is more suitable to deploy and to deal with this problem, since it provides more secure and intelligent data storage system via physical entities instead of software based algorithms as in open PDS. Each PDC actually serves as a secured as well as centralized physical space for each SecNet user where his/her data lives in. 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.

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. Fortunately, the rise of Block chain technologies bring in a hopeful, efficient and effective way to enable trust data sharing in trust less environment, which can help AI make more accurate decisions due to the real big data collected from more places in the Internet. SecNet leverages the emerging block chain technologies to prevent the abuse of data, and to enable trusted data sharing in trust-less or even untrusted environment. For instance, it can enable cooperations between different edge computing paradigms to work together to improve the whole system performance of edge networks [19]. The reason why block chain can enable trusted mechanisms is that it can provide a transparent, tamper-proof metadata infrastructure to seriously recode all the usage of data [17]. Thus, SecNet introduces block chain-based data sharing mechanisms with ownership guarantee, where any data ready for sharing should be registered into a block chain, named Data Recording Block chain (DRB), to announce its availability for sharing. Each access behavior on data by other parties (not the data owner) should also be validated and recorded in this chain. In addition, the authenticity and integrity of data can only be validated by DRB as well. Besides, SecNet enables economic incentive between different entities if they share data or exchange security service, by embedding smart contract on data to trigger automatic and tamper-proof value exchange.

In this way, SecNet guarantees the data security and encourages data sharing throughout the CPS. Furthermore, data is the fuel of AI [11], and it can greatly help to improve the performance of AI algorithms if data can be efficiently networked and properly fused. Enabling data sharing across multiple service providers can be a way to maximize the utilization of scattered data in separate entities with potential conflicts of interest, which can enables a more powerful AI. Given enough data and block chain based smart contract [20] on secure data sharing, it is not surprised that AI can become one of the most powerful technologies and tools to improve cyber security, since it can check huge amount of data more quickly to save time, and identify and mitigate threats more rapidly, and meanwhile give more accurate prediction and decision support on security rules that a PDC should deploy.

Besides, embedded with Machine Learning [21] inside, AI can constantly learn patterns by applying existing data or artificial data generated by GAN [22] to improve its strategies over time, to strengthen its ability on identifying any deviation on data or behaviors on a 24/7/365 basis. SecNet can apply these advanced AI technologies into its Operation Support System (OSS) to adaptively identify more suspicious data-related behaviors, even they are never seen before. In addition, swarm intelligence can be used in SecNet to further improve the data security, by collecting different security knowledge from huge amount of intelligent agents scattered everywhere in the CPS, with the help of trusted exchange mechanisms for incentive tokens [23].

[2] LITERATURE SURVEY

Data security is among key concerns of any network architectures, and is the base for AI algorithms to improve due to its requirement for huge amount of data from as much as possible places in Internet. Meanwhile, with a more powerful AI, data security can be further protected at a higher level as an enhanced AI can figure out advanced and complicated threats more easily than normal AI. To enhance the security of data in CPS, numbers of efforts are conducted. The work in [3] presents an architecture named Amber to enable decoupling data from the web applications, which gives control ability to web users over their personal data, as well as provides a powerful web-wide query function to search personal data. To extend the decoupling mechanism of data and applications from only web services to all kinds of applications, the research group from the Media Lab in Massachusetts Institute of Technology designs the open PDS [5], acting as a secured virtual space for users to collect, store and manage their data, separating all kinds of applications from operating on data directly. In addition, openPDS introduces a new service paradigm named SafeAnswer, to dynamically protect data privacy by reducing the dimensions of personal data.

Besides, the emerging block chain technology provides an efficient and effect way to guarantee the security of data in CPS, by providing tamper-proof and traceable recording features as well as incentive mechanisms. The authors in [8] develop the Origin Chain system to realize the transparency and tamper-proof features of the metadata when the supply chain traces products. Origin Chain enables all related parties to obtain the same trusted data and adapt to dynamic environment and regulations. The authors in [10] propose a block chain-based MeDShare system to effectively manage and protect medical records, as well as share medical data among cloud repositories, with guarantees on data provenance, auditing and controlling. The work in [17] overviews the background of block chain and Intrusion Detection System (IDS) in details, and discusses how to apply block chain technologies to IDS, as well as gives reasonable guesses about possible hidden dangers in this direction. Besides, the work in [15] designs a block chain-based incentive mechanism for crowd sensing applications, with privacy preserving and data security guaranteeing. Furthermore, AI is also a promising way to enhance data security in CPS, since it can deeply analyze huge amount of data, learn hidden patterns and then make accurate predictions, with the help of availability of enormous data and increased computational power.

The work in [11] has made a detailed overview about the use of AI for big data as well as the use of big data for AI, and also put forward some development directions including how to improve the data security by AI. The work in [16] highlights AI can gain better performance if provided huge amount of data to achieve a better base model, and appeals to develop more efforts for building larger valuable datasets, to empower the AI for better security of data. Furthermore, the work in [21] overviews and presents a

comprehensive survey on AI methods for cyber security. In addition, the work in [20] aims at creating a market where participants can exchange machine learning modes for rewards, making AI more practical and accessible to everyone, and thus providing more AI solutions
for better security of data 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 block chain to meet demands of certain applications, or by integrating AI algorithms 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 combining the power of AI and block chain together 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. It is worth noting that SecNet is different from HyperNet [1]. For instance, firstly, AI in HyperNet mainly acts as the virtual personal assistant to protect privacy of a single PDC user while AI in SecNet is also in charge of generating artificial data for training more robust security rules, which can be used to enhance AI again. Secondly, how to securely sharing security rules with the help of a detailed on-chain smart contract is given in SecNet, yet Hypernet lacks. In addition, SecNet aims at achieving a more secure cyberspace by sharing not only user data
but also security rules produced by AI, while Hypernet only aims at securely sharing user data. Last but not least, PDC is only one of the data storing solutions for SecNet yet is the only solution for Hypernet.

In this paper, the Existing System, 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.

In this paper, the Proposed System, 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
a) 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.
b) 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 Block chain to display share data otherwise ignore request.
c) 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. To implement this project author has taken medical data sharing example and I am also using same concept to build this paper.

[3] SYSTEM ARCHITECTURE

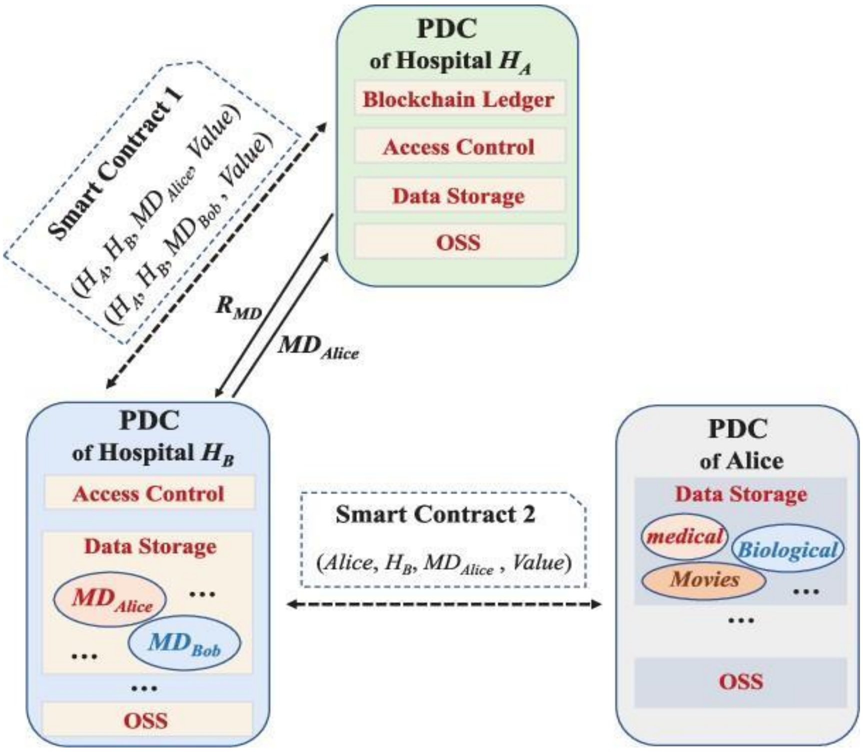


Fig. 1 System Architecture

As shown in Figure, if the hospital HA wants to use Alice's medical data MD Alice , which is currently stored in another hospital HB , to support a very important medical experiment. HA needs to access its PDC PA , and then send the data request RMD containing the metadata/identifier IDR to the PDC PB belonged to HB.

When PB receives the RMD from PA , the Access Control module analyzes the RMD with the help of ASC module in OSS, and meanwhile record this request behavior to the Block chain Ledger, waiting for state synchronization. After the RMD is excluded from malicious access behavior according to the analyzing result from ASC as well as its sub module GAN, the Access Control module communications with the Data Storage module for the RMD and then triggers the on-chain smart contract SC1 between HB and HA on the requested data MDAlice , and maybe necessarily triggers the smart contract SC2 between HB and Alice. The former regulates the value that HA should pay for the requested data from HB , and the latter for the value that HB should transfer to Alice since the ownership of MDAlice belongs to her. When HA receives the requested data MDAlice , corresponding value (e.g., tokens, coins, electric cash) is transferred from HA to HB and from HB to Alice, according to the smart contracts SC1 and SC2 respectively. That is, HB gains rewards by providing storing service for Alice's medical data, and Alice is also paid by allowing her medical data to be shared with HB

[4] IMPLEMENTATION

4.1 Software Environment

In this paper, we are developed the application the following are the Software Requirements are

1. Python
2. Anaconda
3. Pycham

4.2 Modules Information:

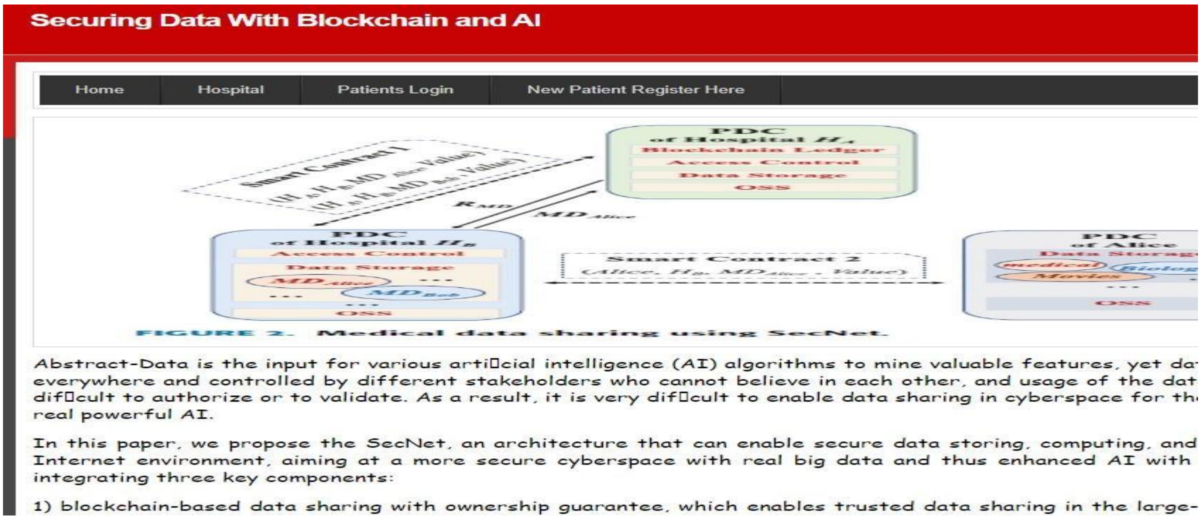
In this paper we are implemented, this work consists of two modules are

i) 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 Block chain 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.

ii) 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.

4.3 Screen Shots



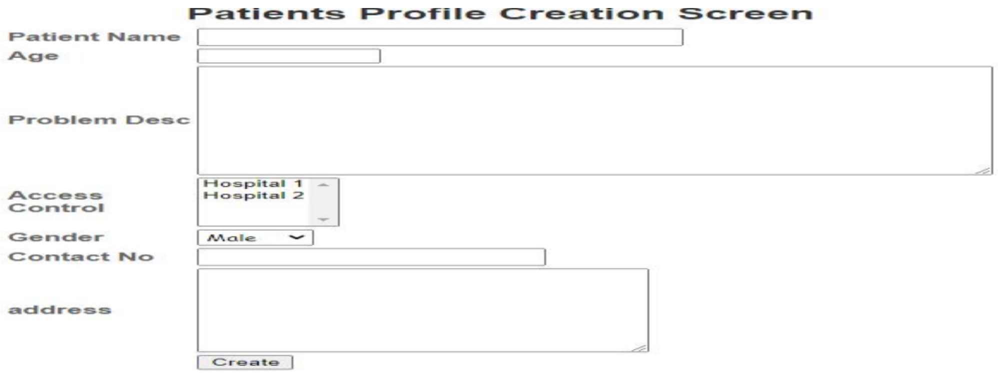
Abstract-Data is the input for various artificial intelligence (AI) algorithms to mine valuable features, yet da everywhere and controlled by different stakeholders who cannot believe in each other, and usage of the dat difficult to authorize or to validate. As a result, it is very difficult to enable data sharing in cyberspace for th real powerful AI.

In this paper, we propose the SecNet, an architecture that can enable secure data storing, computing, and Internet environment, aiming at a more secure cyberspace with real big data and thus enhanced AI with integrating three key components:

1) blockchain-based data sharing with ownership guarantee, which enables trusted data sharing in the large-

Fig. 2 Registration Page

By using Securing Data With Block Chain and AI we can Register.



Patients Profile Creation Screen

Patient Name

Age

Problem Desc

Access Control: Hospital 1, Hospital 2

Gender: Male

Contact No

address

Fig. 3 Patients Profile Creation Screen

To enter the patient Details we can use this patients Profile Creation Screen

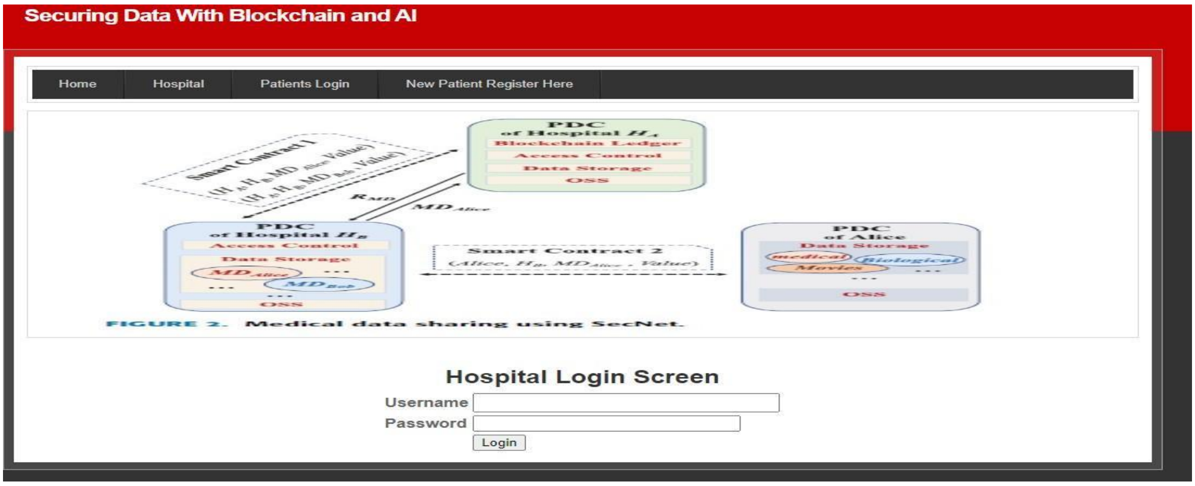


FIGURE 2. Medical data sharing using SecNet.

Hospital Login Screen

Username

Password

Fig.4 Hospital Login Screen

By entering User name and Password , we can Login into the Hospital Brochure

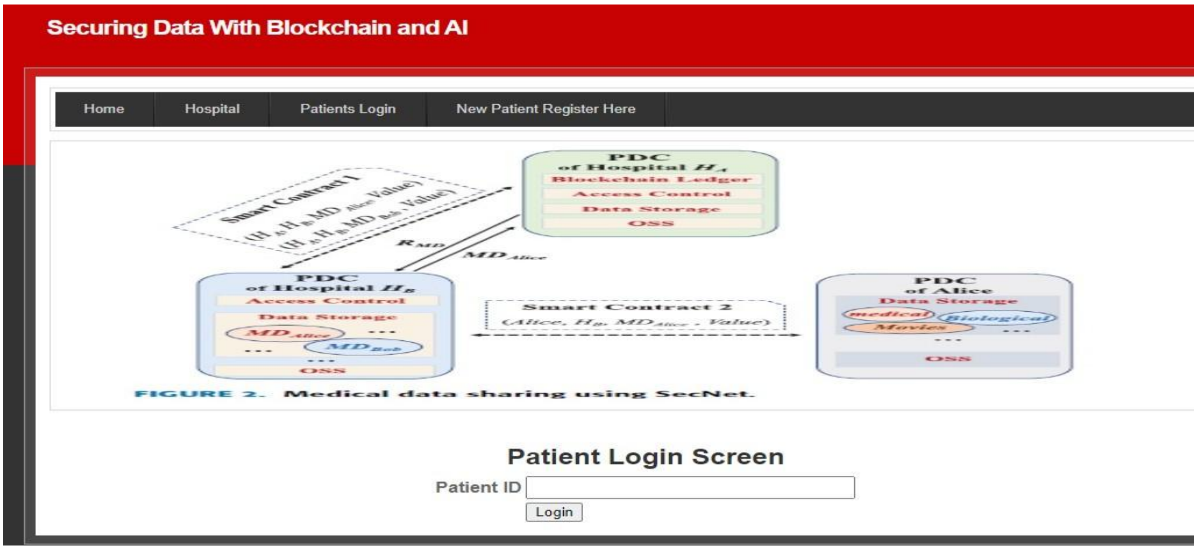


FIGURE 2. Medical data sharing using SecNet.

Patient Login Screen

Patient ID

Fig. 5 Patient Login Screen

By entering Patient ID , we can get Patient details.

[5] CONCLUSION AND FUTURE WORK

In order to leverage AI and block chain to fit the problem of abusing data, as well as empower AI with the help of block chain 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 block chain technologies, and AI-based secure computing platform as well as block chain-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. 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 block chain 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).

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.

[11] D. E. O’Leary, ‘‘Artificial intelligence and big data,’’ IEEE Intell. Syst., vol. 28, no. 2, pp. 96–99, Mar. 2013.

[12] A. Halevy, P. Norvig, and F. Pereira, ‘‘The unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.

[13] Z. Cai and X. Zheng, ‘‘A private and efficient mechanism for data uploading in smart cyber-physical systems,’’ IEEE Trans. Netw. Sci. Eng., to be published. doi: 10.1109/TNSE.2018.2830307.

[14] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, ‘‘BlockChain: A dis- tributed solution to automotive security and privacy,’’ IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, Dec.2017.

[15] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, ‘‘A blockchain based privacy preserving incentive mechanism in crowd sensing applications,’’ IEEE Access, vol. 6, pp. 17545–17556, 2018.

[16] C. Sun, A. Shrivastava, S. Singh, and A. Gupta, ‘‘Revisiting unreasonable effectiveness of data in deep learning era,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Oct. 2017, pp. 843– 852.

[17] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, ‘‘When intrusion detection meets block chain technology: A review,’’ IEEE Access, vol. 6, pp. 10179–10188, 2018.

[18] J.-H. Lee, ‘‘BIDaaS: Blockchain based ID as a service,’’ IEEE Access, vol. 6, pp. 2274–2278, 2017.

[19] K. Wang, H. Yin, W. Quan, and G. Min, ‘‘Enabling collaborative edge computing for software defined vehicular networks,’’ IEEE Networks., vol. 32, no. 5, pp. 112–117, Sep./Oct. 2018.

[20] A. B. Kurtulmus and K. Daniel, ‘‘Trustless machine learning con- tracts; evaluating and exchanging machine learning models on the ethereum blockchain,’’ 2018, arXiv:1802.10185. [Online]. Available: https://arxiv.org/abs/1802.10185

[21] A. L. Buczak and E. Guven, ‘‘A survey of data mining and machine learning methods for cyber security intrusion detection,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[22] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, ‘‘Generative adversarial networks,’’ 2014, arXiv:1406.2661. [Online]. Available: https://arxiv.org/abs/1406.2661

[23] E. C. Ferrer, ‘‘The blockchain: A new framework for robotic swarm systems,’’ 2017, arXiv:1608.00695. [Online]. Available: https://arxiv.org/abs/1608.00695

[24] IPFS. Accessed: Jun. 5, 2019. [Online]. Available: https://ipfs.io/

[25] S. T. Zargar, J. Joshi, and D. Tipper, ''A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,'' IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.

[26] A. Praseed and P. S. Thilagam, ''DDoS attacks at the application layer: Challenges and research perspectives for safeguarding Web applications,'' IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 661–685, 1st Quart., 2019.

[27] J. Benet, ''IPFS—Content addressed, Versioned, P2P file system,'' 2014, arXiv:1407.3561. [Online]. Available: https://arxiv.org/abs/1407.3561

[28] G. Wood, ''Ethereum: A secure decentralised generalised transaction ledger,'' Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[29] SK Althaf Hussain Basha, B Sasidhar, "A Review on the Challenges of E-Commerce Security Issues, Privacy, Trust and Solutions", International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad, 2013.

[30] SK Althaf Hussain Basha, B Sasidhar, " The Effect of E-Commerce Applications on Marketers and Consumers: A Case Study ", International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad,2013.

[31]SK. Althaf Husain Basha, Sk Nikhath, P Yejdani Khan . "Safety Fear/Attacks Current in Cloud Environment", Volume 4, Issue 2, November 2019, pp. 324-330, International Journal of Recent Issues on Computer Science & Electronics(IJRICSE)

[32] Jinka Sreedhar , SK Althaf Hussain Basha, Pammi Pavan Kumar, , "Innovative Techniques and Technologies in Translation in a Multilingual Context -2012", Third International Conference on Translation, Technology and Globalization in Multilingual Context, ITA, NewDelhi.

[33] B Sasidhar, SkAlthaf Hussain Basha, A.Govardhan, , " Data Mining Techniques using in E – Learning Domain", Published in proceeding of National Conference on "Data Mining and Data Warehousing" (DMDW2009) atMRCET,Secunderabad,121-127,2009.

[34] G.V.S.Raju, Sk Altaf Hussain Basha, K.Venkata Subbaih, A.V.N. Sharma, "Facilities Layout Optimization using Genetic Algorithm", International Conference on Advanced Computing Technologies (ICACT 2008), GRIET,Hyderabad,32-36,2008, ISSN: 9788178003

[35] Shaik Yasmin Sulthana , SK Althaf Hussain Basha, "IOT Based Shutter Alarm Security System" Journal of Engineering Sciences (JES), Vol.11, Issue 7,July/2020, pp.1035-1045, ISSN No:0377-9254.

[36] Sd.Muneer, SK Althaf Hussain Basha,, E.Srinivasa Reddy, I Ramesh Babu," Robust Watermarking Method For Any Images Based On Noise Density" International Journal of Advanced Computing(IJAC), Volume 4,Issue 3&4,2012,pp.114-121,ISSN: 0975-7686.

[37] Dr. G. N. R. PRASAD, "Identification of Bloom's Taxonomy level for the given Question paper using NLP Tokenization technique", Turkish Journal of Computer and Mathematics Education, Vol.12 No.13 (2021), 1872-1875.