JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452

Protecting Information Using Ai And Blockchain

ANANDA R KUMAR MUKKALA
Associate Professor, CSE.
Sreyas Institute of Engineering and Technology, Telangana, India
anandranjit@sreyas.ac.in

KOMMA REDDY SREEJA
Department of CSE,
Sreyas Institute of Engineering and Technology, Telangana, India
sreejakreddy01@gmail.com

P KEERTHI REDDY
Department of CSE,
Sreyas Institute of Engineering and Technology, Telangana, India
keerthireddypeddamaru@gmail.com

BOLLAMPALLY SHRIYA REDDY
Department of CSE,
Sreyas Institute of Engineering and Technology, Telangana, India
shriyareddy131@gmail.com

MOHAMMED AZHAN AHMED
Department of CSE,
Sreyas Institute of Engineering and Technology, Telangana, India
azhan.ahmed80@gmail.com

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18**.**

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: 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

1.1 PROBLEM STATEMENT

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452

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.

1.2 OBJECTIVE

With the development of information technologies, the trend of integrating cyber, physical and social (CPS) systems to a highly united 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.

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.

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 order of magnitude more scale, even the simplest AI algorithm currently (e.g., perceptions 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 block chain-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 openPDS [5] and the Private Data Centre (PDC) from HyperNet [1], SecNetnally 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 openPDS. 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 ne-grained management on access behaviours 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 stake- holders 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 Blockchain technologies bring in a hopeful, efficient and effective way to enable trust data sharing in trust- less

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452

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 blockchain 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 cooperation's between different edge computing paradigms to work together to improve the whole system performance of edge networks [19]. The reason why blockchain can enable trusted mechanisms is that it can provide a transparent, tamper-proof metadata infrastructure to seriously recode all the usage of data

Thus, SecNet introduces blockchain-based data sharing mechanisms with ownership guarantee, where any data ready for sharing should be registered into a blockchain, named Data Recording Blockchain (DRB), to announce its availability for sharing. Each access behaviour 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 enable a more powerful AI. Given enough data and blockchain- 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 cybersecurity, 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 pat- terns 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 behaviours 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 behaviours, 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].

PROPOSED SYSTEM CONFIGURATION

2.1 EXSISTING SYSTEM

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. 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.

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.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452

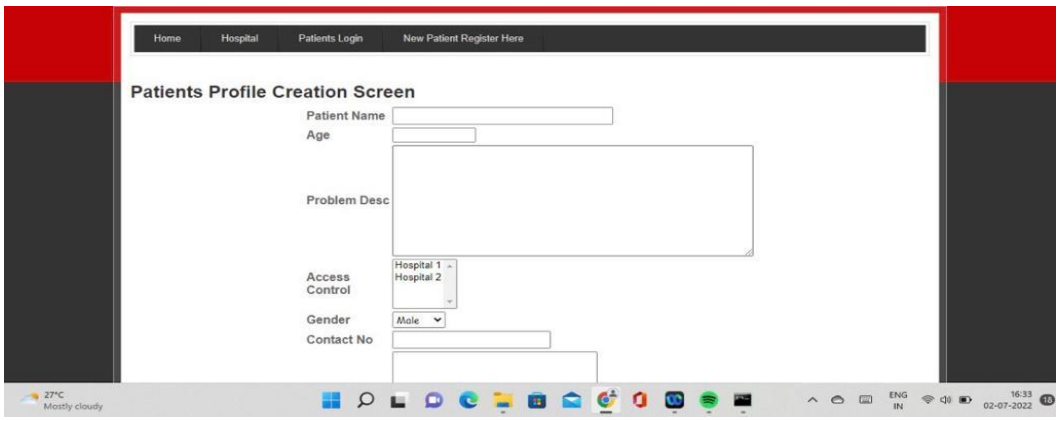
2.2 PROPOSED SYSTEM

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 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.
2) 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 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, 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 project.

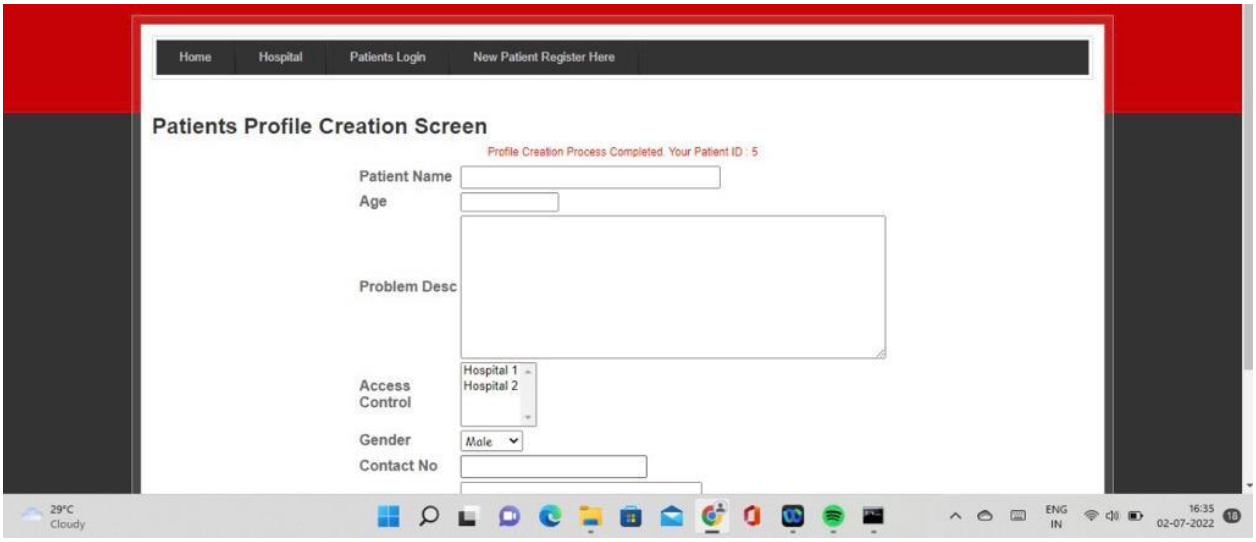
RESULTS



SCREENSHOT.7.1

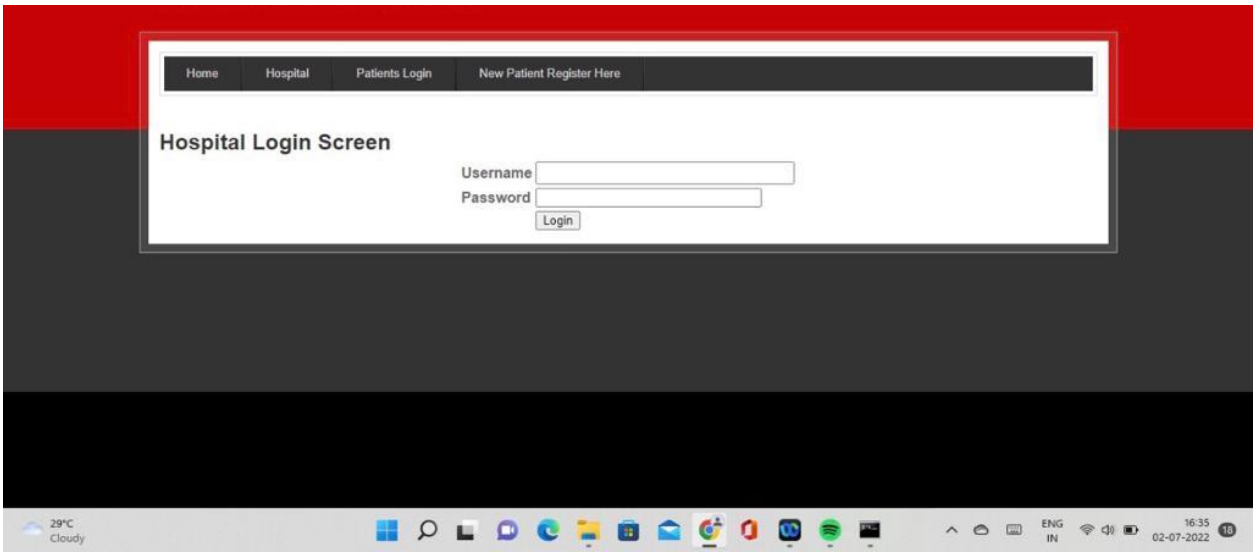
In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452



SCREENSHOT.7.2

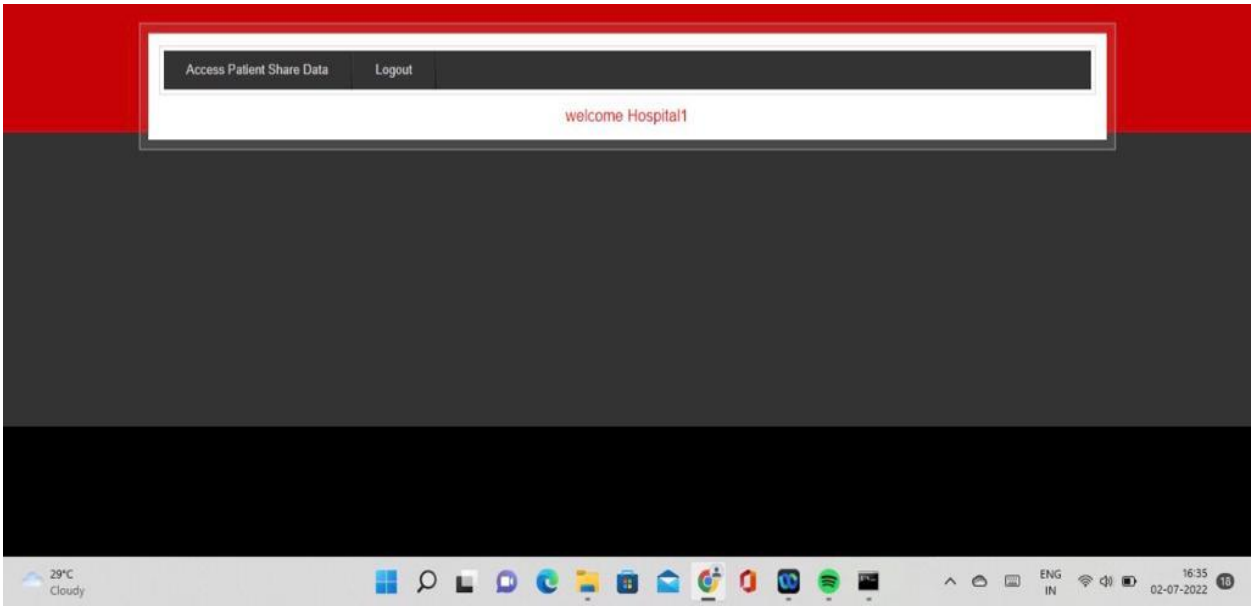
In above screen one patient is created with patient ID 5 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1



SCREENSHOT.7.3

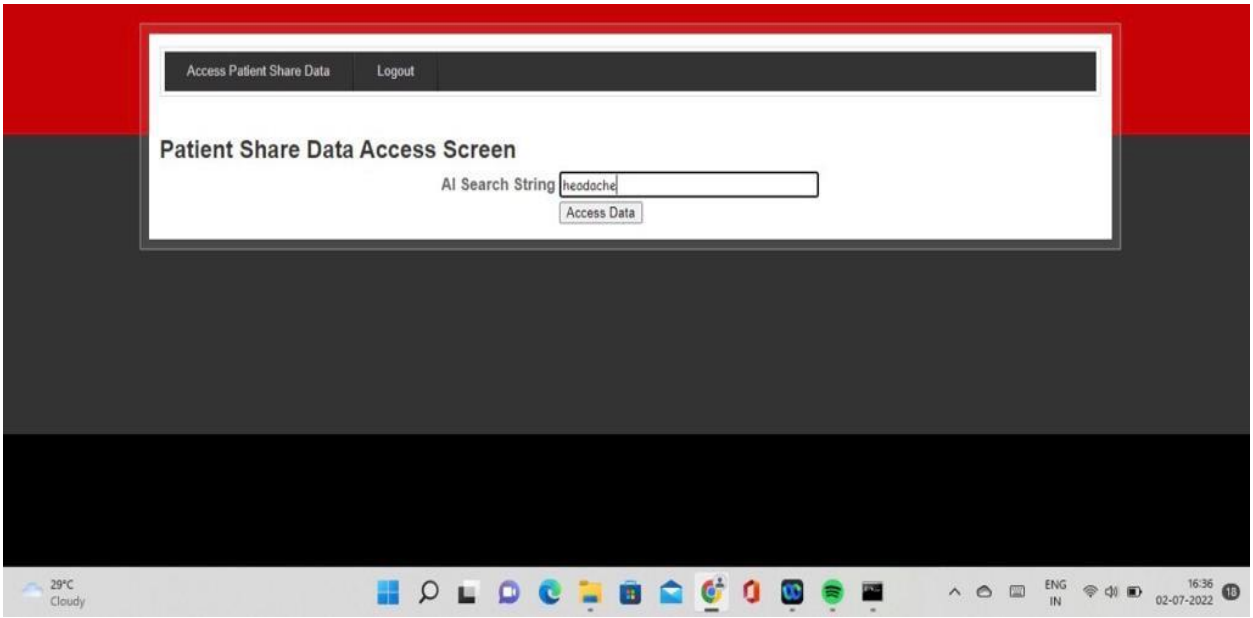
In above screen to login as Hospital1 click on 'Hospital' link to get above screen. Use 'Hospital1' as username and 'Hospital1' as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452



SCREENSHOT.7.4

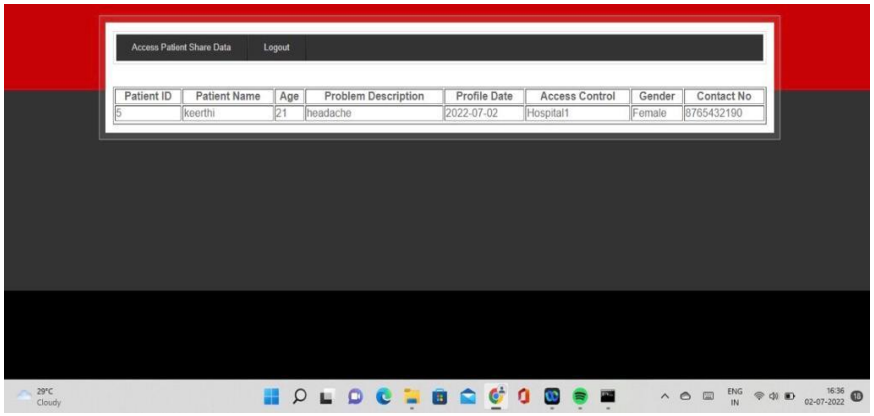
In above screen click on 'Access Patient Share Data' link to search for patient details



SCREENSHOT.7.5

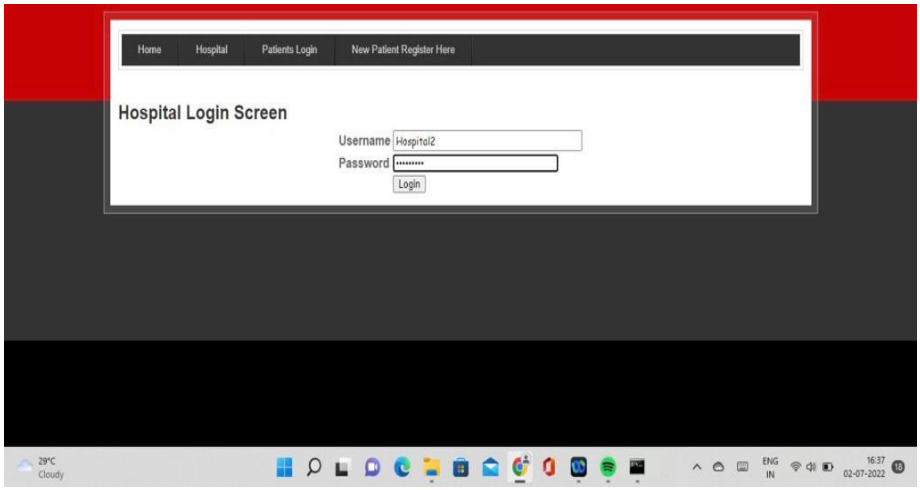
In above screen I want to search for all patients who are suffering from 'pain' and then click on 'Access data' button to get below screen

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452



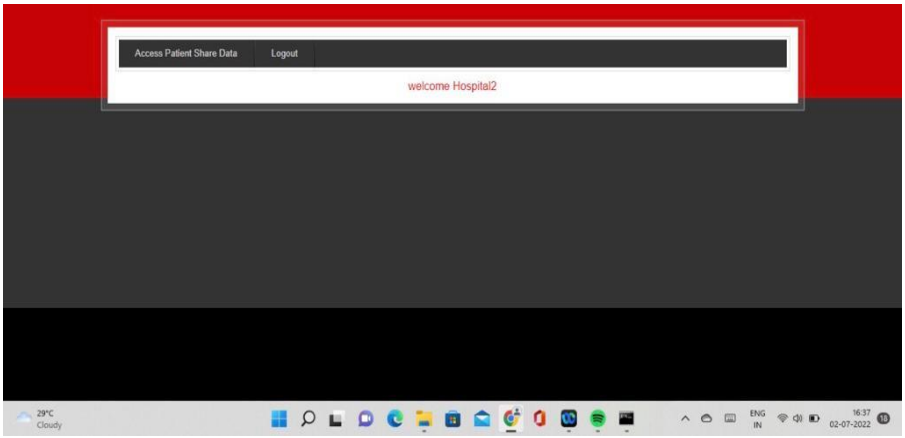
SCREENSHOT.7.6

In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'



SCREENSHOT.7.7

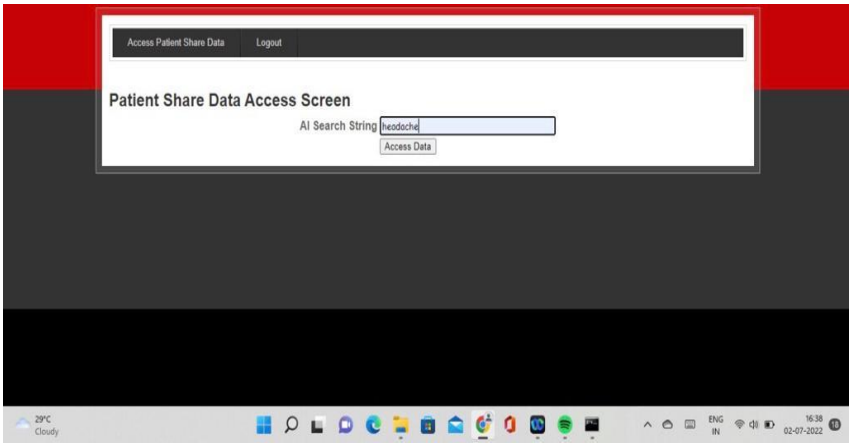
In above screen 'Hospital2' is login, after login will get below screen



SCREENSHOT.7.8

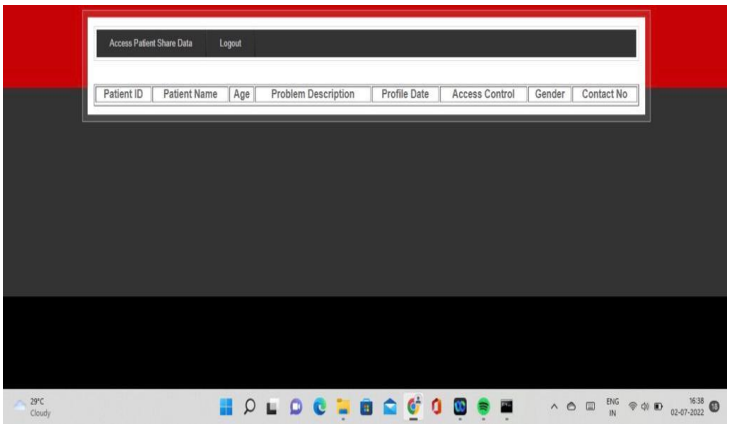
Now click on 'Access Patient Share Data' link and search for same pain disease

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452



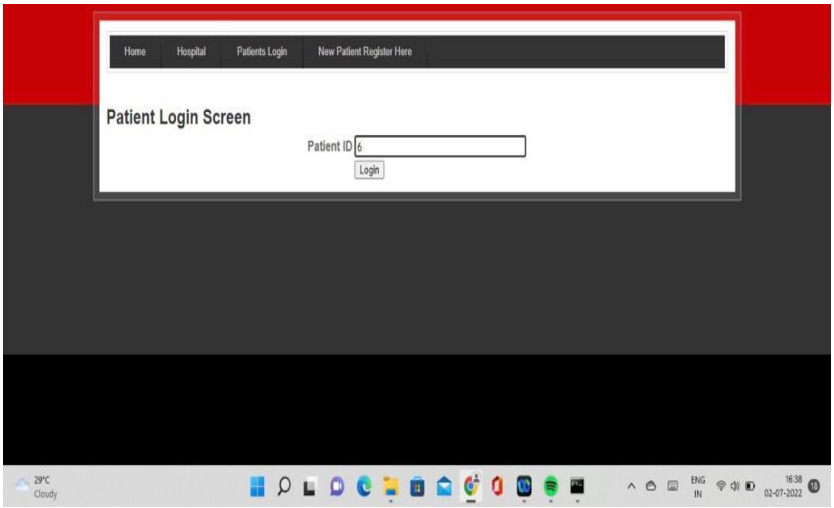
SCREENSHOT.7.9

For above query will get below result



SCREENSHOT.7.10

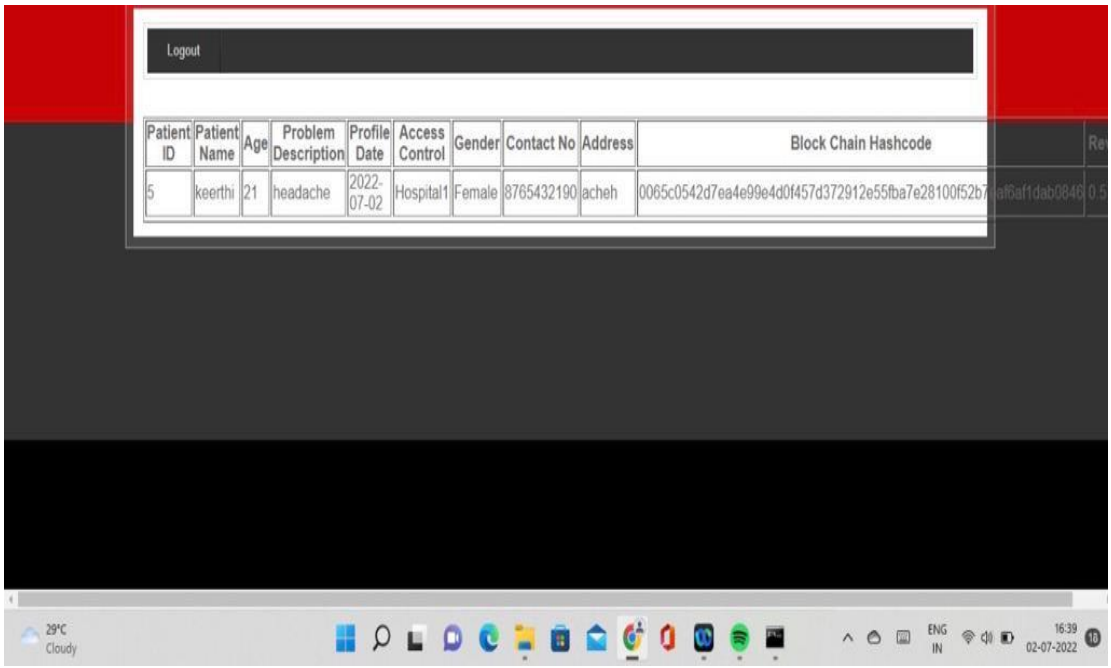
In above screen no patient details are showing as Hospital2 not having permission. So block chain allow only those users to access data who has permission. Now logout and login as patient by entering patient id in below screen



SCREENSHOT.7.11

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 513-522
https://publishoa.com
ISSN: 1309-3452

After login will get below details for patient 1



SCREENSHOT.7.12

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 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.

8.2 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).

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. 112117, 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. 16561665, 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. 16.
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. 3442, 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. 4453, 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. 5561, 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. 2127, 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. 814, 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. 1475714767, 2017.
11. D. E. O'Leary, ``Articial intelligence and big data," IEEE Intell. Syst., vol. 28, no. 2, pp. 9699, Mar. 2013.