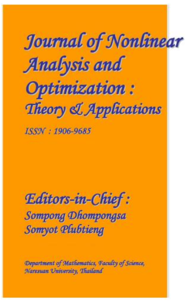
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685

Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng

Department of Mathematics, Faculty of Science,
Naresuan University, Thailand

DATA SECURITY USING BLOCK CHAIN AND AI

Dr.Manyam sukesh, Associate Professor CSE, Vaagdevi College of Engineering(Autonomous), India

N.Sowmya , UG Student ,CSE, Vaagdevi College of Engineering (Autonomous), India

K.Amulya , UG Student , CSE, Vaagdevi College of Engineering (Autonomous), India

D.Thirumal , UG Student ,CSE, Vaagdevi College of Engineering(Autonomous),India

A.Sai Nithesh, UG Student ,CSE, Vaagdevi College of Engineering (Autonomous), 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 ***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.

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 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 [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 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 [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[4], 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.

2. LITERATURE SURVEY

With the development of the Internet of Things, a complex CPS system has emerged and is becoming a promising information infrastructure[5]. 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[6], 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[7].

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 [8]. 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 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 [9]. 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 [10].

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[11]. 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 [12]. 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.

Today's companies collect immense amounts of personal data and enable wide access to it within the company [13]-[16]. 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. PROBLEM STATEMENT

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[17]. 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 [18].

4. PROPOSED 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.

To overcome from above issue author has describe concept called Private Data Centres (PDC) with Blockchain and AI technique[19] to provide security to user's data. In this technique 3 functions will work which describe below

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 [20]-[24]. In Blockchain object user will add/subscribe share data and give permission.

Artificial Intelligence: AI-based secure computing platform to produce more intelligent security rules, which helps to constructa more trusted cyberspace [25]. 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 [26].

5. METHODOLOGY

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 [27].

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 [28], if hospital has access permission then it will display those patients records to that hospital.

6. IMPLEMENTATION

Modules Information:

This project consists of two modules

1.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.

2.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.

Below is the code example to create Block chain object with patient data

```
blockchain = Blockchain() //creating block chain object

x ='{"Patient_id":"'+str(count)+'", "patient_name":"'+name+'", "age":"'+age+'",
"problem_desc":"'+problem+'", "profile_date":"'+str(current_time)+'",
"access_data":"'+str(access)+'","gender":"'+gender+'"}' //creating access with input data

blockchain.add_new_transaction(json.loads(x)) //adding transaction to blockchain

hash = blockchain.mine()//mining transaction to generate hash value
```

In above code see comment to understand

7. OUTPUT SCREENS

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

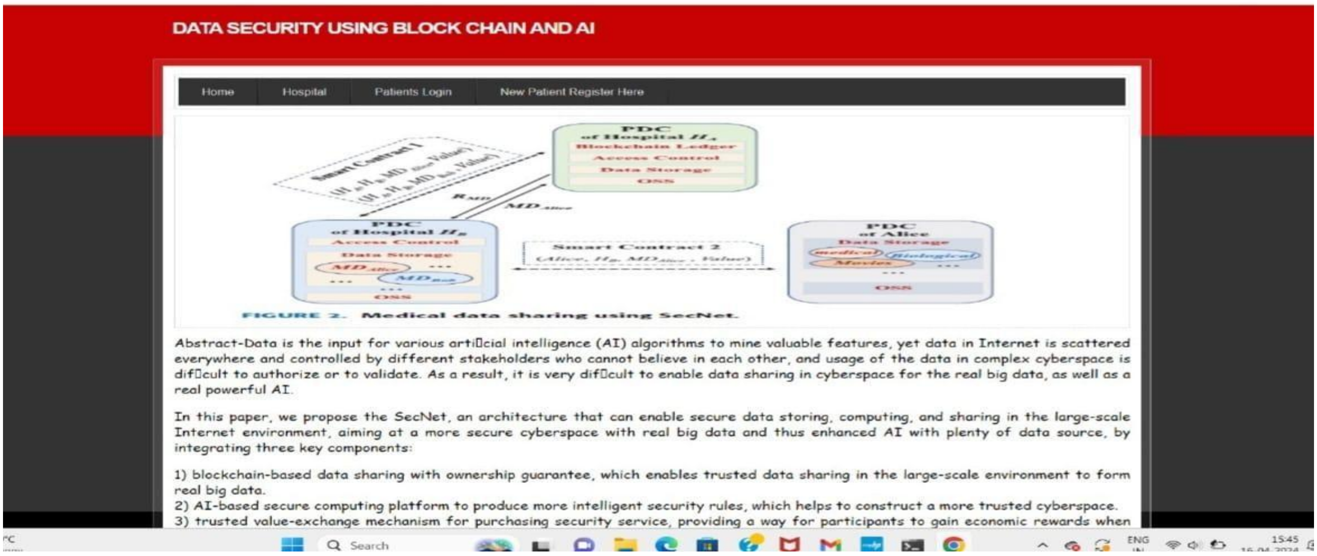


FIGURE 2. Medical data sharing using SecNet.

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

In above screen click on ‘New Patient Register Here’ link to get below screen

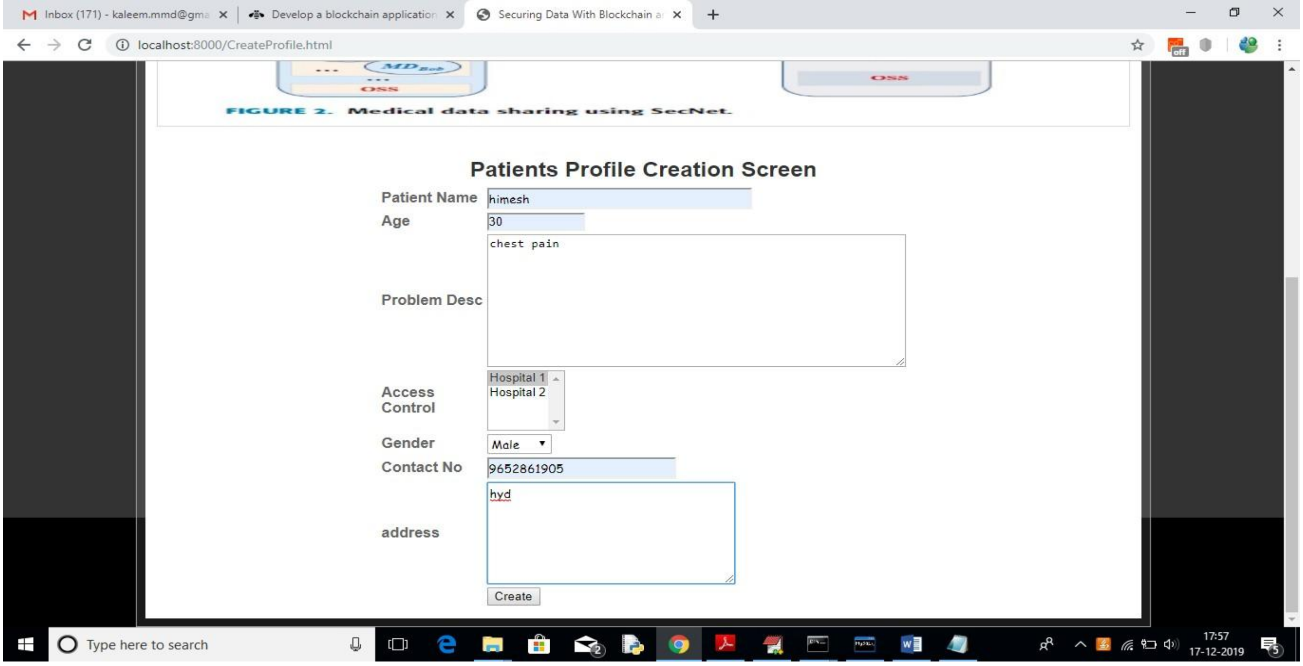

Inbox (171) - kaleem.mmd@gma
Develop a blockchain application
Securing Data With Blockchain a
localhost:8000/CreateProfile.html
MD_Bob
OSS
Type here to search
17:57
17-12-2019

FIGURE 2. Medical data sharing using SecNet.

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

Create

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

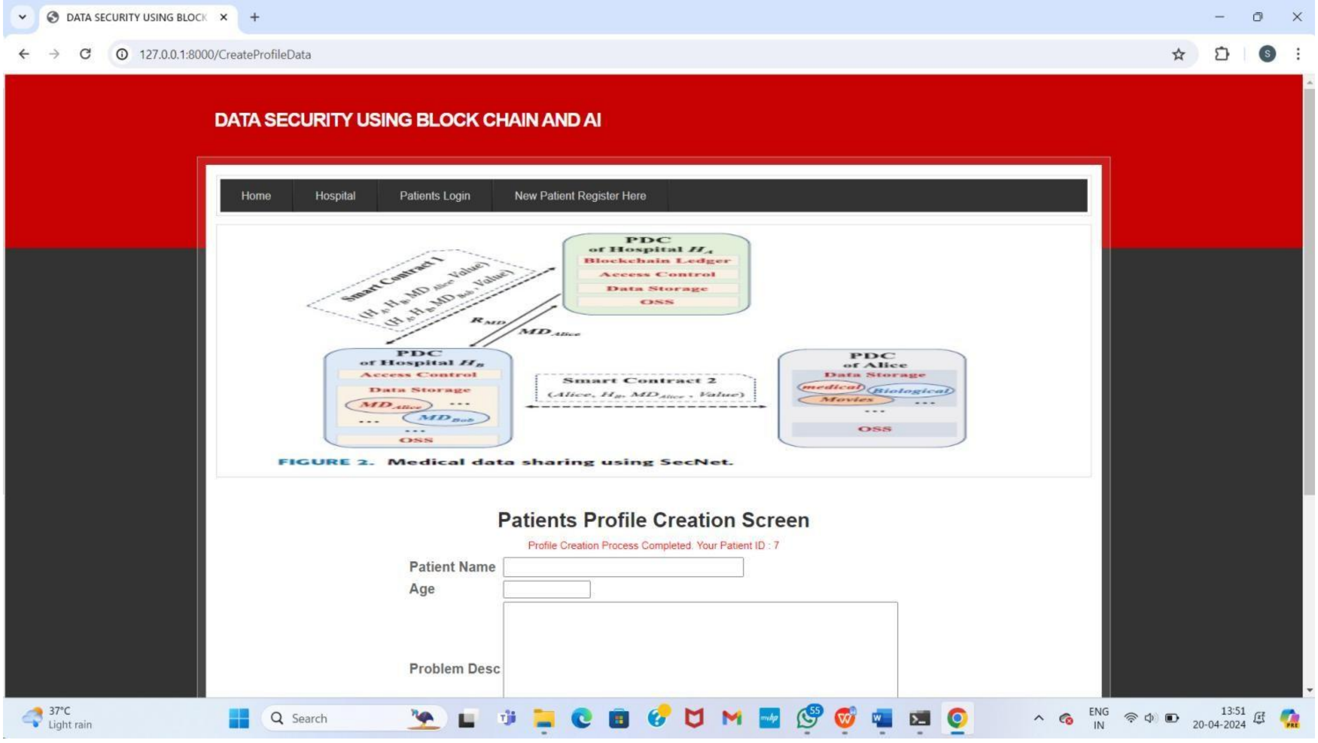


FIGURE 2. Medical data sharing using SecNet.

Patients Profile Creation Screen

Profile Creation Process Completed. Your Patient ID : 7

Patient Name

Age

Problem Desc

In above screen one patient is created with patient ID 7 and now Hospital 1 can login and search and access this patient data as patient has given permission to Hospital1

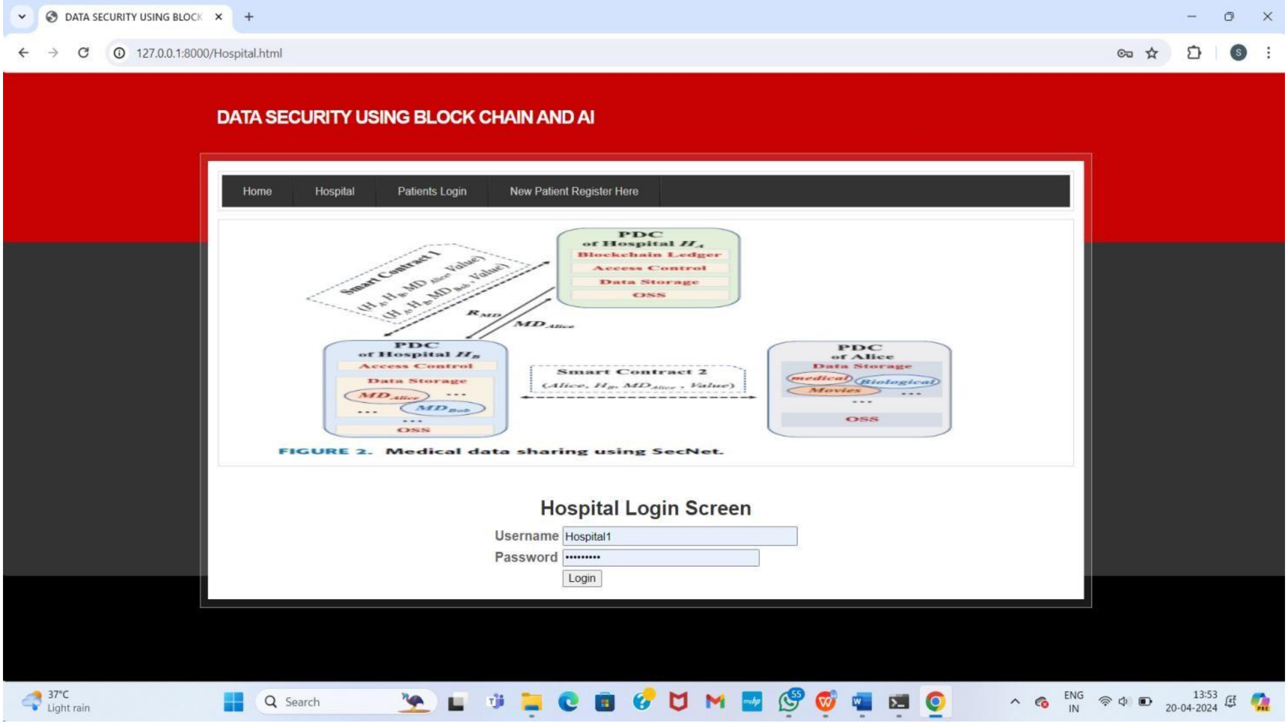


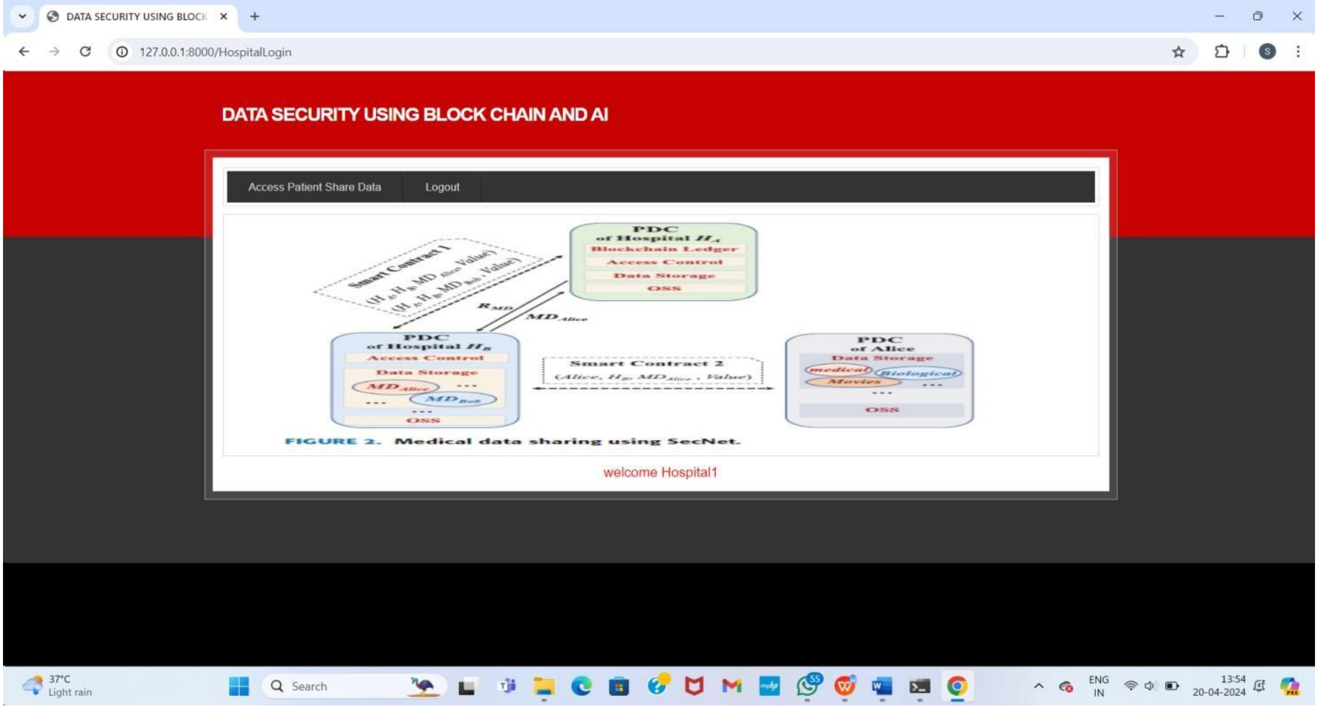
FIGURE 2. Medical data sharing using SecNet.

Hospital Login Screen

Username Hospital1

Password ••••••••

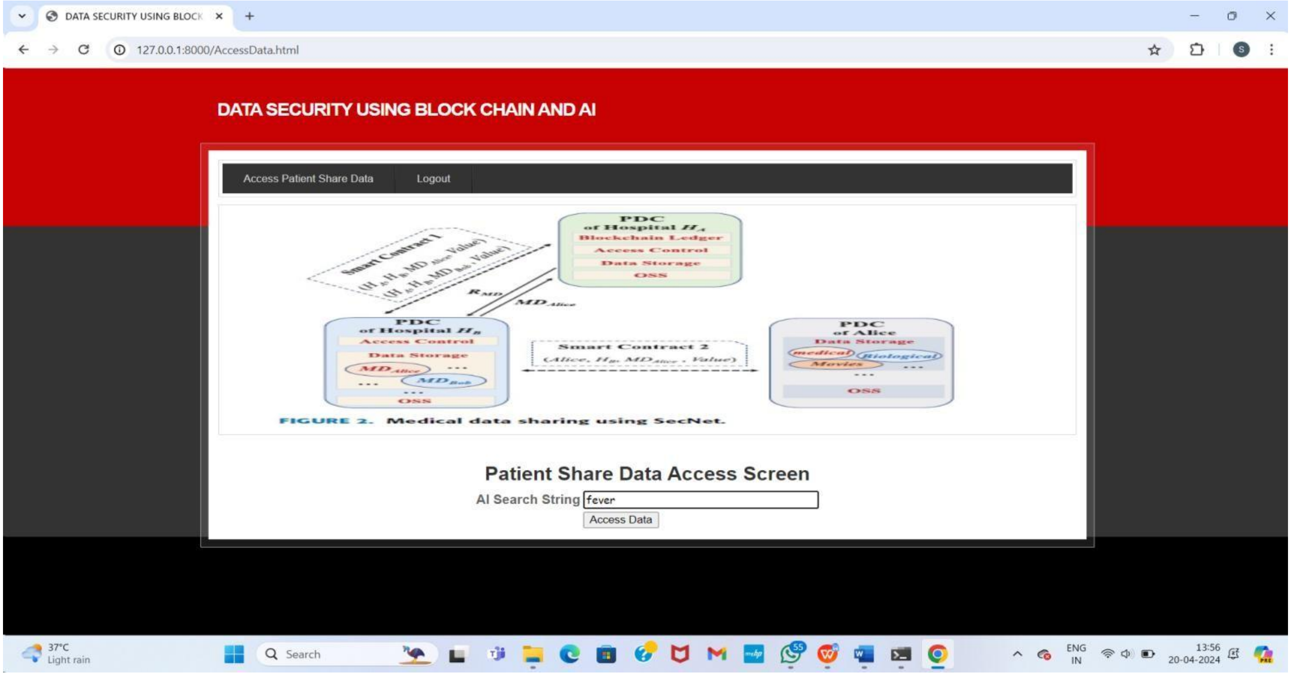
In above screen to login as Hospital1 click on ‘Hospital’ link to get above screen. Use ‘Hospital1’ as username and ‘Hospital1’ as password to login as Hospital1 and use Hospital2 to login as Hospital2. After login will get below screen



DATA SECURITY USING BLOCK CHAIN AND AI

welcome Hospital1

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

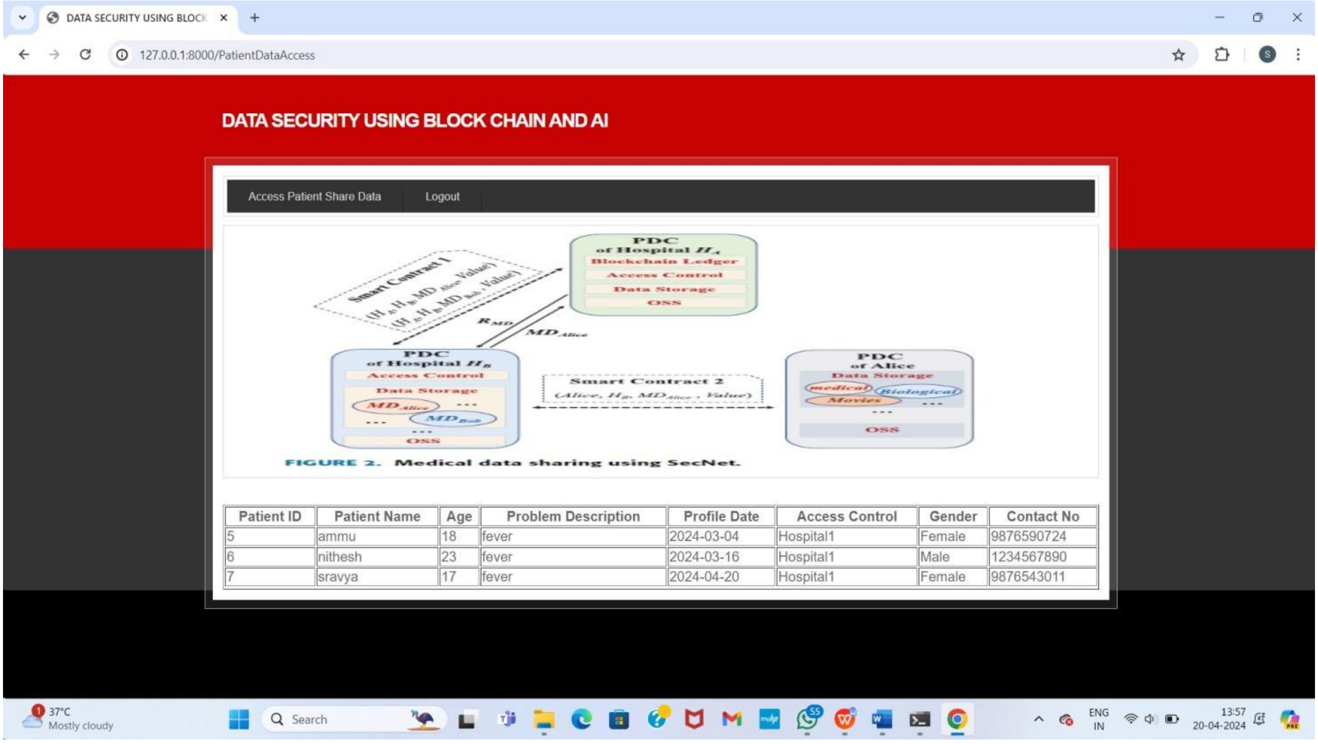


DATA SECURITY USING BLOCK CHAIN AND AI

Patient Share Data Access Screen

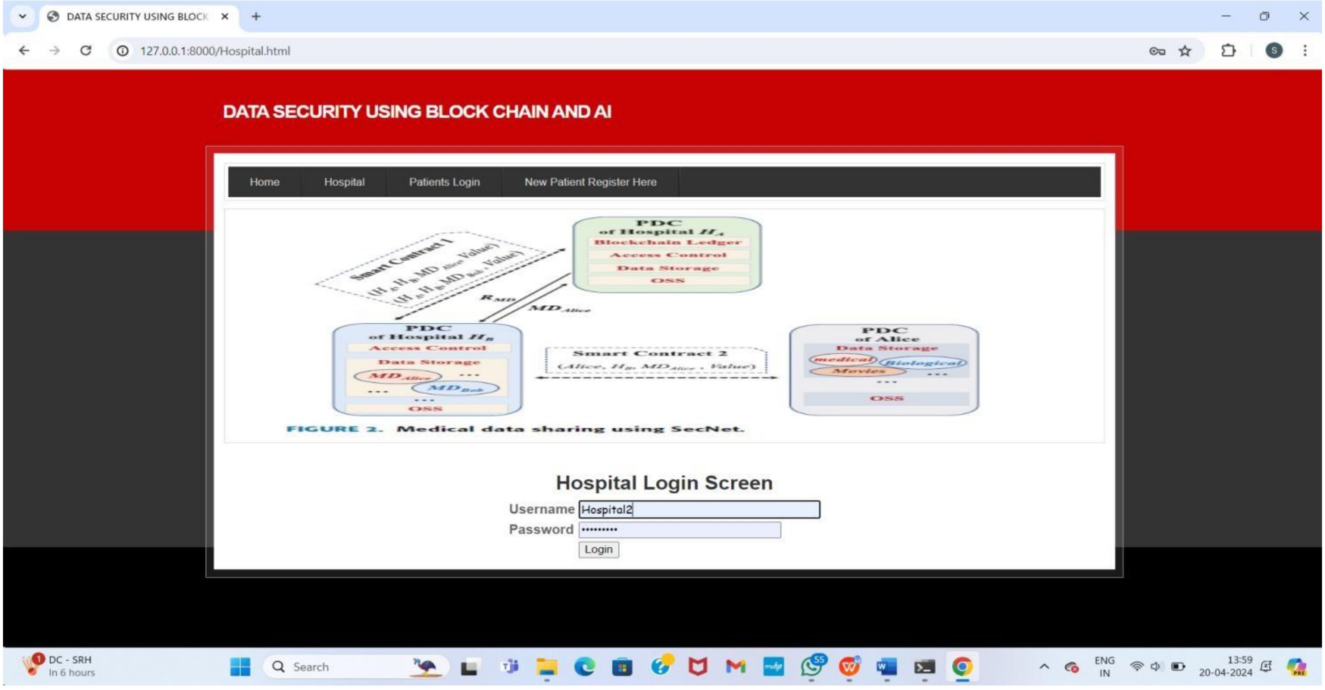
AI Search String: fever

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


DATA SECURITY USING BLOCK
127.0.0.1:8000/PatientDataAccess
DATA SECURITY USING BLOCK CHAIN AND AI
Access Patient Share Data
Logout
FIGURE 2. Medical data sharing using SecNet.
37°C
Mostly cloudy
Search
13:57
20-04-2024

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No
5	ammu	18	fever	2024-03-04	Hospital1	Female	9876590724
6	nithesh	23	fever	2024-03-16	Hospital1	Male	1234567890
7	sravya	17	fever	2024-04-20	Hospital1	Female	9876543011

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’


DATA SECURITY USING BLOCK
127.0.0.1:8000/Hospital.html
DATA SECURITY USING BLOCK CHAIN AND AI
Home
Hospital
Patients Login
New Patient Register Here
FIGURE 2. Medical data sharing using SecNet.
DC - SRH
In 6 hours
Search
13:59
20-04-2024

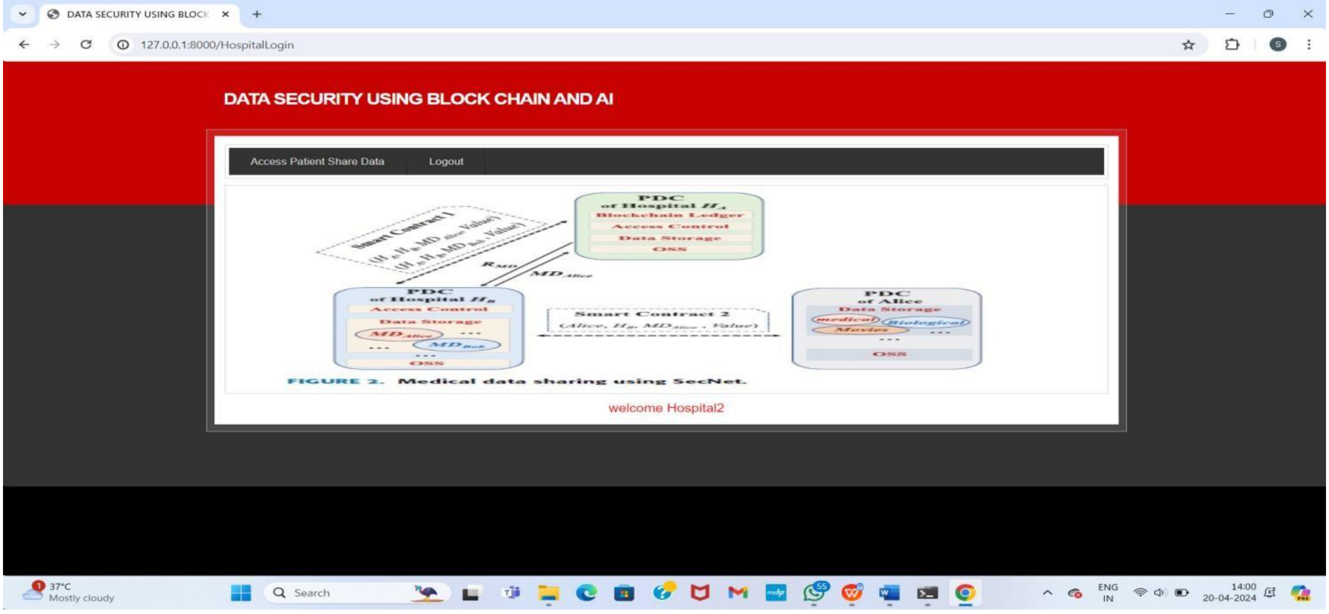
Hospital Login Screen

Username Hospital2

Password ••••••••

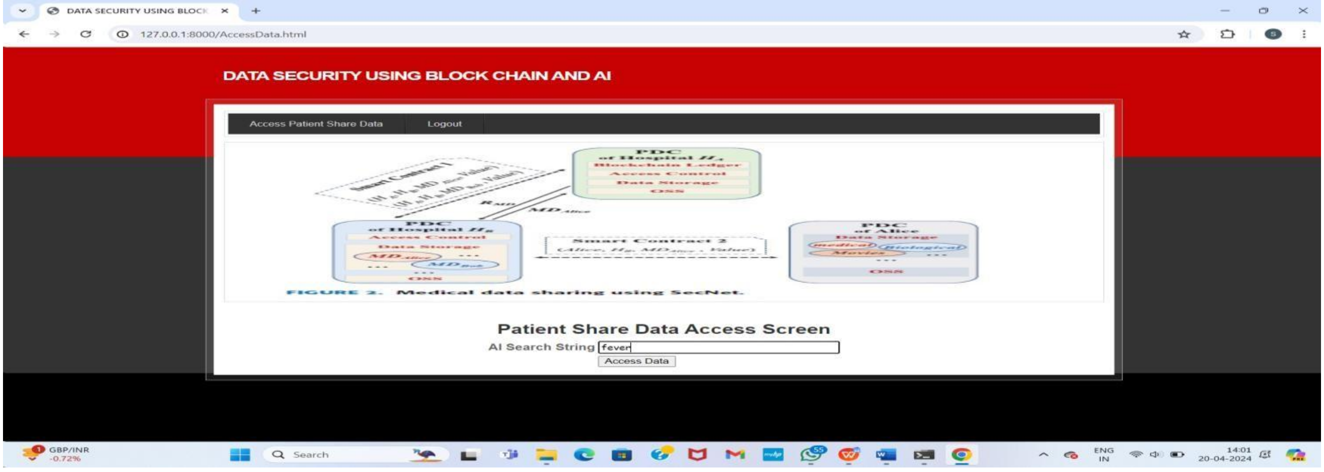
Login

In above screen ‘Hospital2’ is login, after login will get below screen


DATA SECURITY USING BLOCK
127.0.0.1:8000/HospitalLogin
DATA SECURITY USING BLOCK CHAIN AND AI
Access Patient Share Data
Logout
FIGURE 2. Medical data sharing using SecNet.

welcome Hospital2

Now click on ‘Access Patient Share Data’ link and search for same fever disease

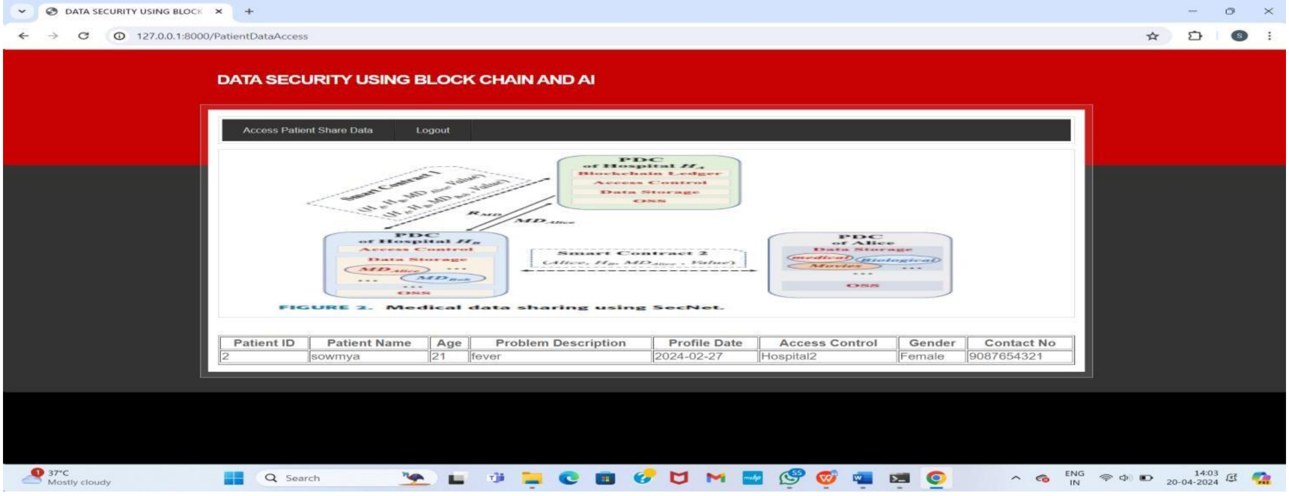

DATA SECURITY USING BLOCK
127.0.0.1:8000/AccessData.html
DATA SECURITY USING BLOCK CHAIN AND AI
Access Patient Share Data
Logout
FIGURE 2. Medical data sharing using SecNet.

Patient Share Data Access Screen

AI Search String: fever

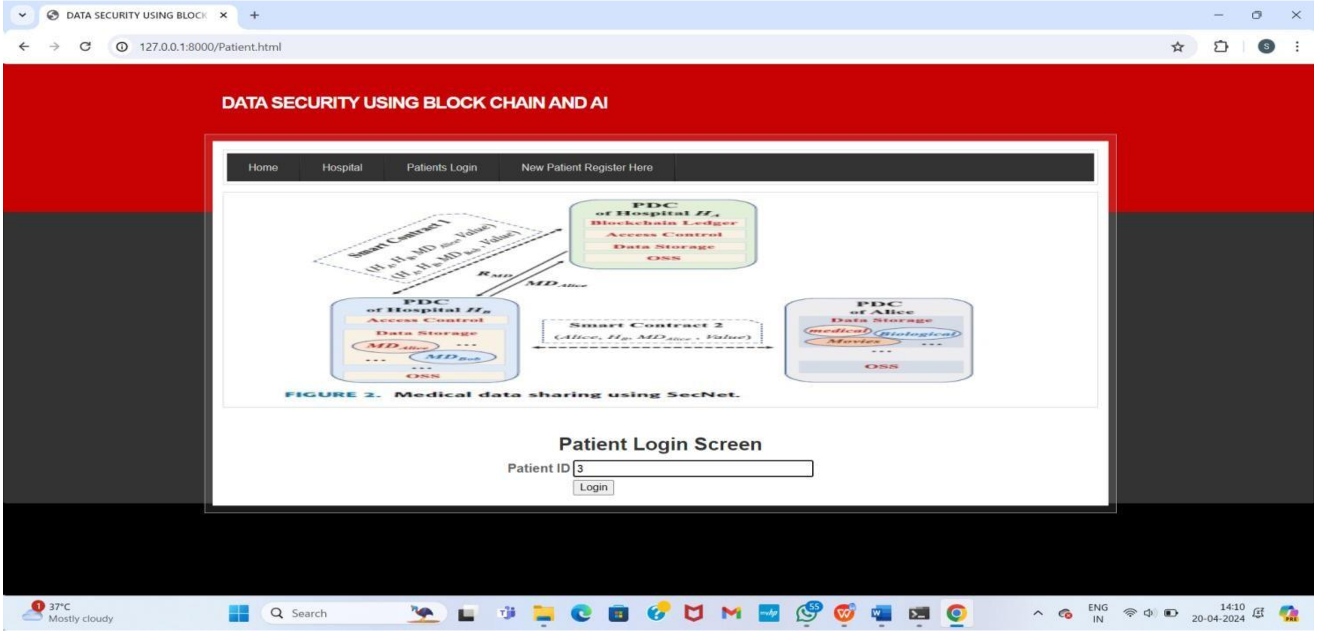
Access Data

For above query will get below result


DATA SECURITY USING BLOCK
127.0.0.1:8000/PatientDataAccess
DATA SECURITY USING BLOCK CHAIN AND AI
Access Patient Share Data
Logout
FIGURE 2. Medical data sharing using SecNet.

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No
2	sowmya	21	fever	2024-02-27	Hospital2	Female	9087654321

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

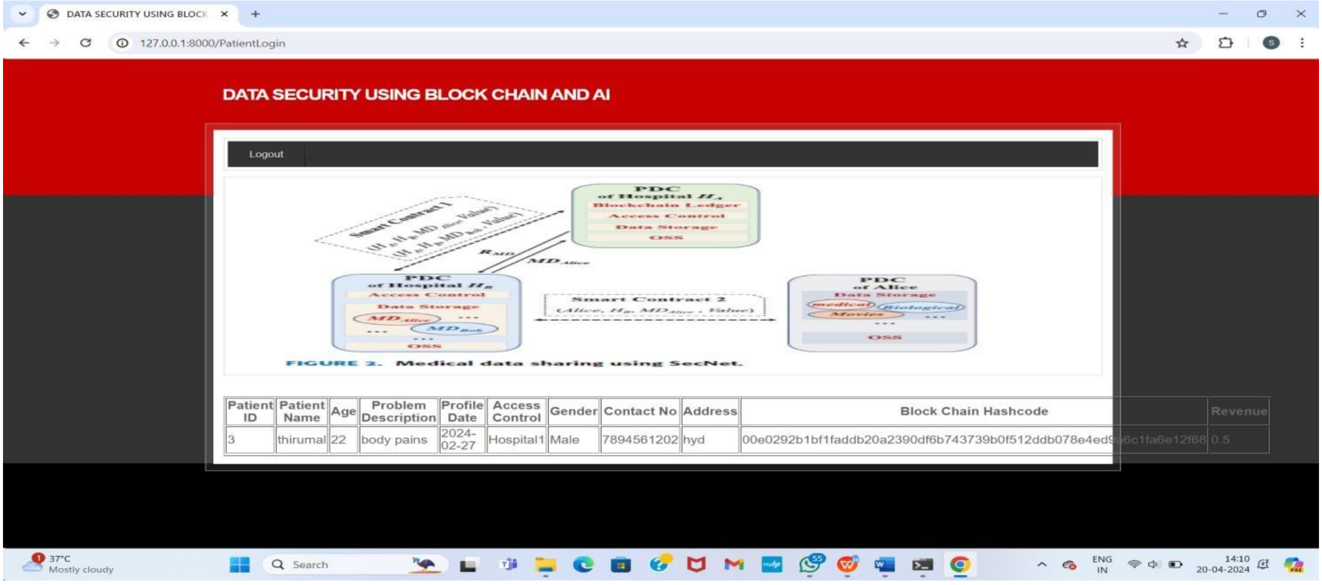


DATA SECURITY USING BLOCK CHAIN AND AI

Patient Login Screen

Patient ID 3

After login will get below details for patient 3



DATA SECURITY USING BLOCK CHAIN AND AI

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No	Address	Block Chain Hashcode	Revenue
3	thirumal	22	body pains	2024-02-27	Hospital1	Male	7894561202	hyd	00e0292b1bf1faddb20a2390df6b743739b0f512ddb078e4ed9a6c1fa6e12f68	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.

8. CONCLUSION AND FUTURE SCOPE

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 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 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 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).

9. 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 distributed 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 crowdsensing 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 blockchain 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 Netw., vol. 32, no. 5, pp. 112–117, Sep./Oct. 2018.

[20] A. B. Kurtulmus and K. Daniel, ‘‘Trustless machine learning contracts; 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 decentralisedgeneralised transaction ledger,'' Ethereum Project Yellow Paper, 2018. Accessed: Jun. 5, 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf