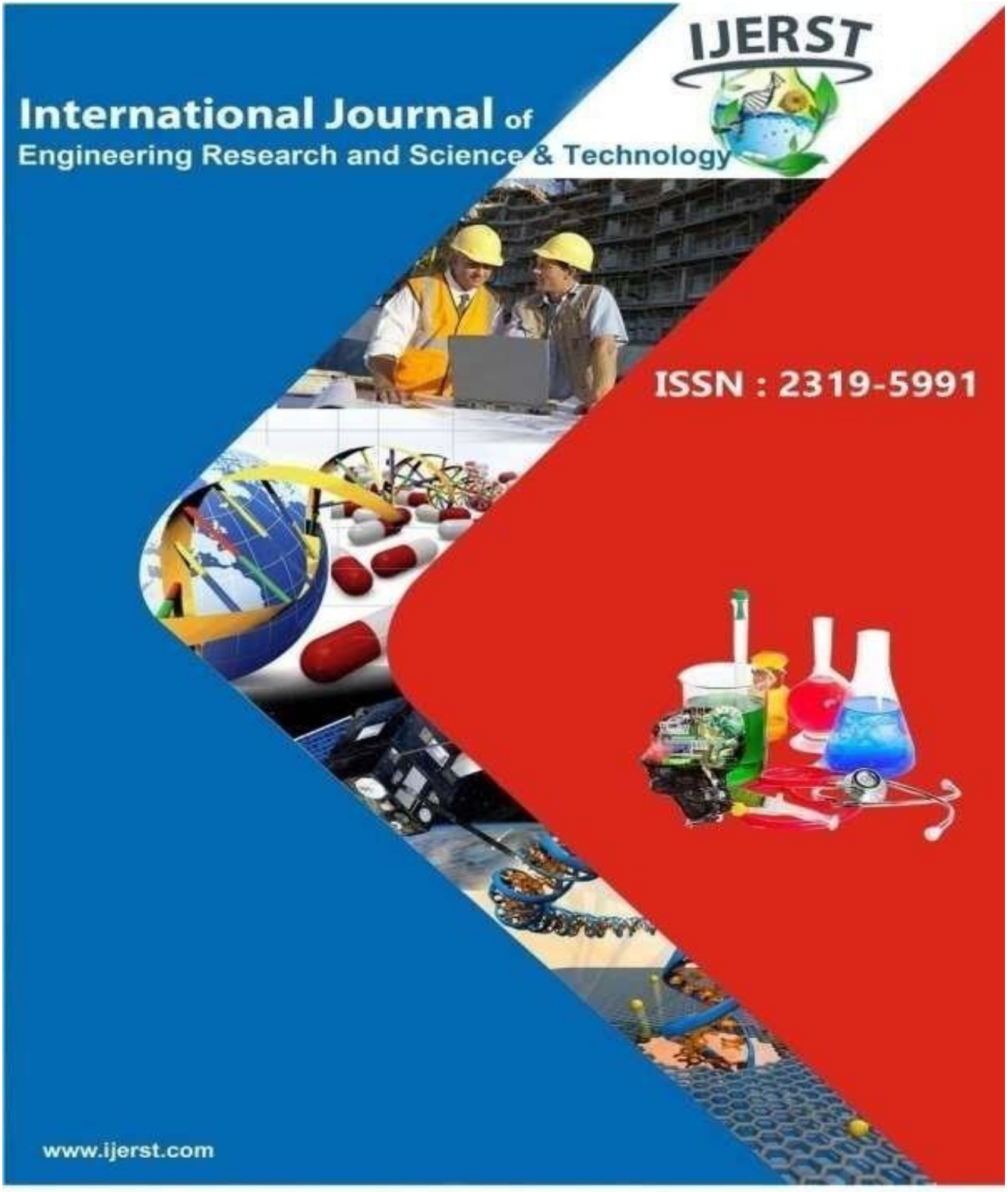


Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

SECURING DATA WITH BLOCKCHAIN AND AI

Manjula. S.D, Maltesh Kamatar, Indira

Assoc. Professor, Asst. Professor, Asst. Professor

manjulasd@pdit.ac.in, maltkpl@pdit.ac.in, indira@pdit.ac.in

Department of CSE, Proudhadevaraya Institute of Technology, Abheraj Baldota Rd, Indiranagar, Hosapete, Karnataka-583225

ABSTRACT

While data is essential for artificial intelligence (AI) algorithms to extract useful characteristics from, it is difficult to authorise or approve data use in complicated cyberspace due to the dispersed nature of the Internet and the fact that its diverse stakeholders do not trust one another. Consequently, enabling data exchange in cyberspace for genuine large data and a real strong AI is quite difficult. In this work, we present SecNet, an architecture that can provide secure data storage, processing, and sharing in a large-scale Internet setting. Our goal is to create a safer cyberspace with true big data, which will lead to improved artificial intelligence with access to a wealth of data. To do this, we integrate three essential components: 1) a blockchain-based data sharing system that ensures ownership of shared data, allowing for trustworthy data sharing in large-scale environments to create real big data; 2) a secure computing platform powered by AI to create smarter security rules, contributing to the development of a more trustworthy cyberspace; 3) a trusted value-exchange mechanism for buying security services, where participants can earn money for sharing their data or services, encouraging data sharing and improving AI performance. Furthermore, we examine SecNet's efficacy from the perspective of economic income and network security, and we talk about its usual use case and its perhaps other deployment method.

Keywords: Block chain, high security, high efficiency.

I. INTRODUCTION

1.Hyperconnected network: A decentralized trusted computing and networking paradigm

With the development of the Internet of Things, a complex CPS system has emerged and is becoming a promising information infrastructure. In the CPS

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

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, 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.

2. Lightweight RFID protocol for medical privacy protection in IoT

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. 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. 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.

3. Amber: Decoupling user data from Web applications

User-generated content is becoming increasingly common on the Web, but

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

current web applications isolate their users' data, enabling only restricted sharing and cross-service integration. 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. 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.

4. Enhancing selectivity in big data

Today's companies collect immense amounts of personal data and enable wide access to it within the company. 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.

II.EXISTING SYSTEM

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. 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 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.

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

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

and thus achieves better performance of AI

III.MODULES EXPLANATION

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.

Securing Data With Blockchain and AI

In cyber world everything is dependent on data and all Artificial Intelligence algorithms discover knowledge from past data only, for example in online shopping application users review data is very important for new comers to take decision on which product to purchase or not to purchase, we can take many examples like health care to know good hospitals or education institutions etc. Not all cyber data can be made publicly available such as Patient Health Data which contains patient disease details and contact information and if such data available publicly then there is no security for that patient data.

Now a days all service providers such as online social networks or cloud storage will store some type of 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

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

3) 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.

4) 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.

5) 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.

To implement this project author has taken medical data sharing example and I am also using same concept to build this project.

Modules Information:

This project consists of two modules

3) 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.

4) 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

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

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

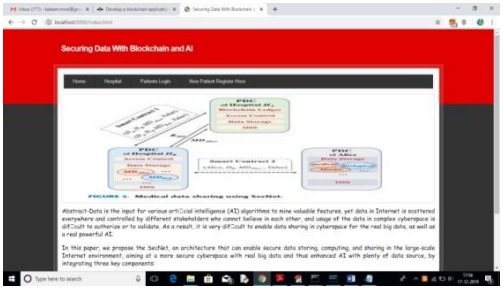
In above code see comment to understand

Screen shots

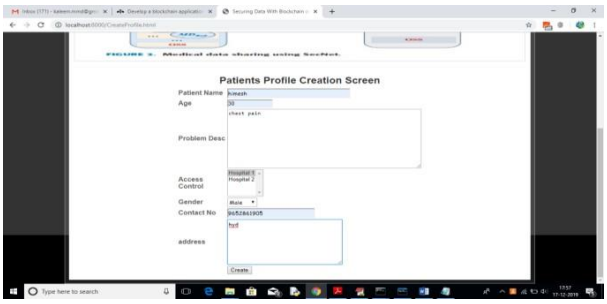
First create database in MYSQL by copying content from 'DB.txt' file and paste in MYSQL.

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



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

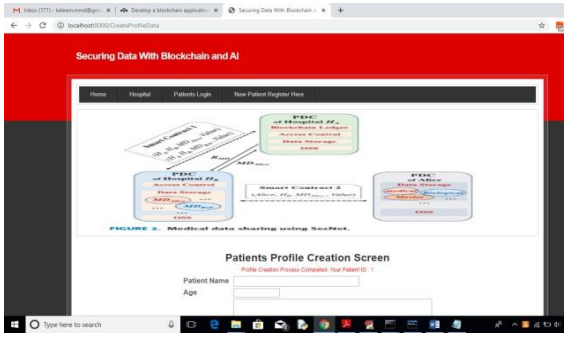


In above screen I am adding patient disease details and selecting 'Hospital1' to share my data and if you want to share with two hospitals then hold 'CTRL' key and select both hospitals to give permission. Now press 'Create' button to create profile

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

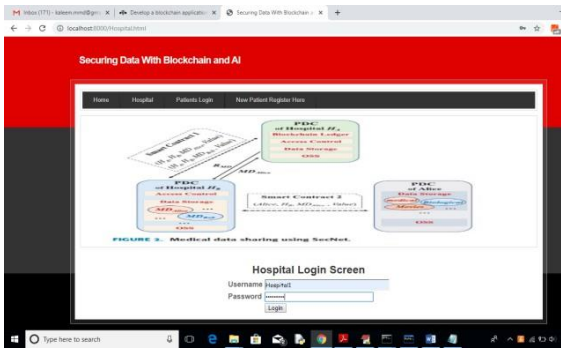
Vol. 19, Issue 3, 2023



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



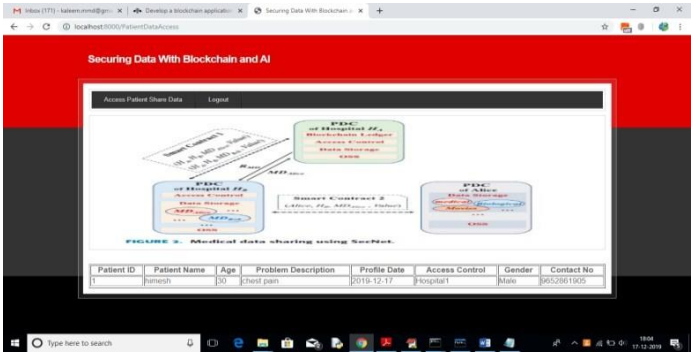
In above screen click on 'Access Patient Share Data' link to search for patient details



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



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

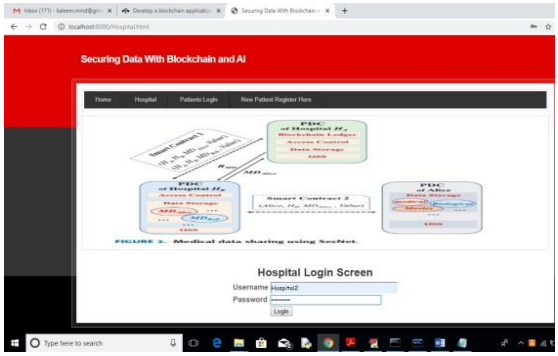


In above screen Hospital1 getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as 'Hospital2'

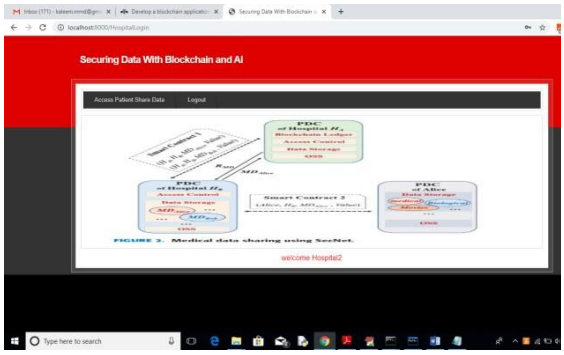
International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023



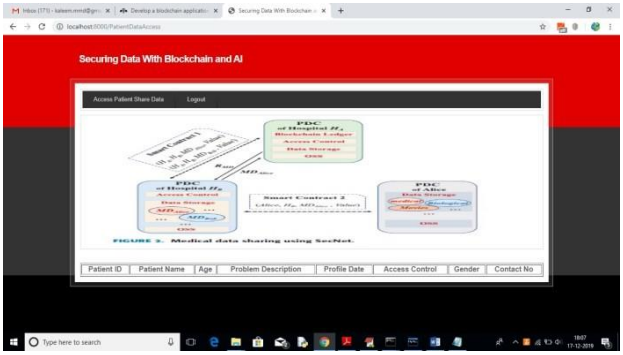
In above screen 'Hospital2' is login, after login will get below screen



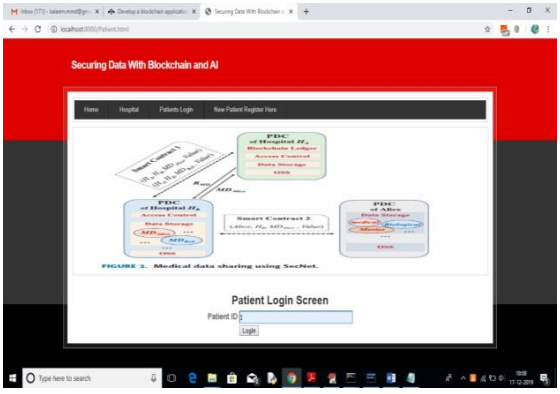
Now click on 'Access Patient Share Data' link and search for same pain disease



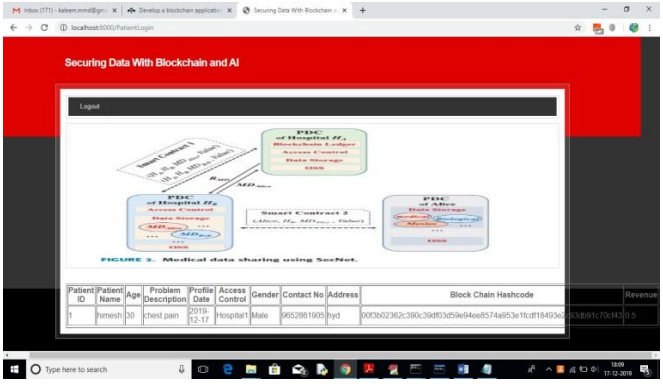
For above query will get below result



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



After login will get below details for patient 1



International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

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.

IV.CONCLUSION

We present the SecNet, a new networking paradigm that prioritises secure data storage, sharing, and computation over communication, as a means to harness AI and blockchain technology to address the issue of data abuse and to enable AI in a trust-less environment to manage data. In order to provide improved network security, SecNet offers data ownership guarantees using blockchain technologies, an AI-based secure computing platform, and an incentive system that is based on blockchain. These features enable a paradigm shift and incentives for data merging, leading to more powerful AI. We also provide other methods of using SecNet's storage function and go over the common use case of SecNet in healthcare systems. We also look at the innovative part about getting people to contribute security rules for a safer network and how it improves the network's susceptibility to DDoS assaults.

V.REFERANCES

[1] Satoshi Nakamoto et al., “Bitcoin: A peer-to-peer electronic cash system.,” 2008.

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in 2017 IEEE international congress on big data (BigData congress). IEEE, 2017, pp. 557–564.

[3] Yu-Pin Lin, Joy R Petway, Johnathen Anthony, Hussnain Mukhtar, ShihWei Liao, Cheng-Fu Chou, and Yi-Fong Ho, “Blockchain: The evolutionary next step for ict e-agriculture,” Environments, vol. 4, no. 3, pp. 50, 2017.

[4] Fthi Arefayne Abadi, Joshua Ellul, and George Azzopardi, “The blockchain of things, beyond bitcoin: A systematic review,” in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 19, Issue 3, 2023

Data (SmartData). IEEE, 2018, pp. 1666–1672.

[5] Feng Tian, "A supply chain traceability system for food safety based on haccp, blockchain & internet of things," in 2017 International conference on service systems and service management. IEEE, 2017, pp. 1–6.

[6] Selena Ahmed and Noah ten Broek, "Blockchain could boost food security," Nature, vol. 550, no. 7674, pp. 43–43, 2017.

[7] Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang, "A blockchain-based supply chain quality management framework," in 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE). IEEE, 2017, pp. 172–176.

[8] Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, and Lejia Shen, "Blockchain technology and its relationships to sustainable supply chain management," International Journal of Production Research, vol. 57, no. 7, pp. 2117–2135, 2019.

[9] Rosanna Cole, Mark Stevenson, and James Aitken, "Blockchain technology: implications for operations and supply chain management," Supply Chain Management: An International Journal, vol. 24, no. 4, pp. 469– 483, 2019.

[10] Jane Thomason, Mira Ahmad, Pascale Bronder, Edward Hoyt, Steven Pocock, Julien Bouteloupe, Katrina Donaghy, David Huysman, Tony Willenberg, Ben Joakim, et al., "Blockchain—powering and empowering the poor in developing countries," in Transforming climate finance and green investment with blockchains, pp. 137–152. Elsevier, 2018.

[11] Diana Kos and Sanneke Kloppenburg, "Digital technologies, hypertransparency and smallholder farmer inclusion in global value chains," Current Opinion in Environmental Sustainability, vol. 41, pp. 56–63, 2019.

[12] Guoqing Zhao, Shaofeng Liu, Carmen Lopez, Haiyan Lu, Sebastian Elgueta, Huilan Chen, and Biljana Mileva Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," Computers in Industry, vol. 109, pp. 83–99, 2019.