International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Securing Data with Blockchain and AI

Kamisetty Vinay

Department of ECE, Sri Indu College of Engineering and Technology
Email Id: *vinayk8188[at]gmail.com*

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.***

Keywords: SectNet, Blockchain, AI, Security

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. 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. 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.

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.

2. Literature Survey

-
- H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing, Hyperconnected network: A decentralized trusted computing and networking paradigm.
- K. Fan, W. Jiang, H. Li, and Y. Yang, Lightweight RFID protocol for medical privacy protection in IoT.
- Amber: Decoupling user data from Web applications. Enhancing selectivity in big data.

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

3. 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. 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 algorithms will gain knowledge from previous data only. As the technology is increasing day by day, some of service providers such online social network or cloud storage will store some type of users data and they can sale that data for their benefits and user has no control on his/her data because the data is saved on third party servers.

Drawbacks:
1) There is no security for the user's data.
2) User has no control on his data.

4. Proposed System

To overcome such issue we are using private data centers with blockchain and AI to provide security to user's data. It contains three functions
1) **Blockchain:** Blockchain based data sharing with user guarantee. In this technique user can give access control it means he give permission to the users who want to see his data and he can deny the permission or access control who don't want to see his information or data. Blockchain object will generate such functions like the user who give permission to the other user, that user only can able to access data.
2) **Artificial Intelligence:** AI based secure computing platform to produce more intelligent security rules, AI helps to construct more secure trusted cyberspace. AI will work like human brain it is responsible to excute logic when the user is requesting to access the data it will check first whether the requested user has permission to access shared data or not if the user has permission then only it allows the user to access the data.
3) **Rewards:** In this technique all users who is sharing data will get rewards upon any user access his data. It provides the way for participants to gain economic rewards when giving out their data. Which promotes the data sharing and thus achieves better performance of AI.

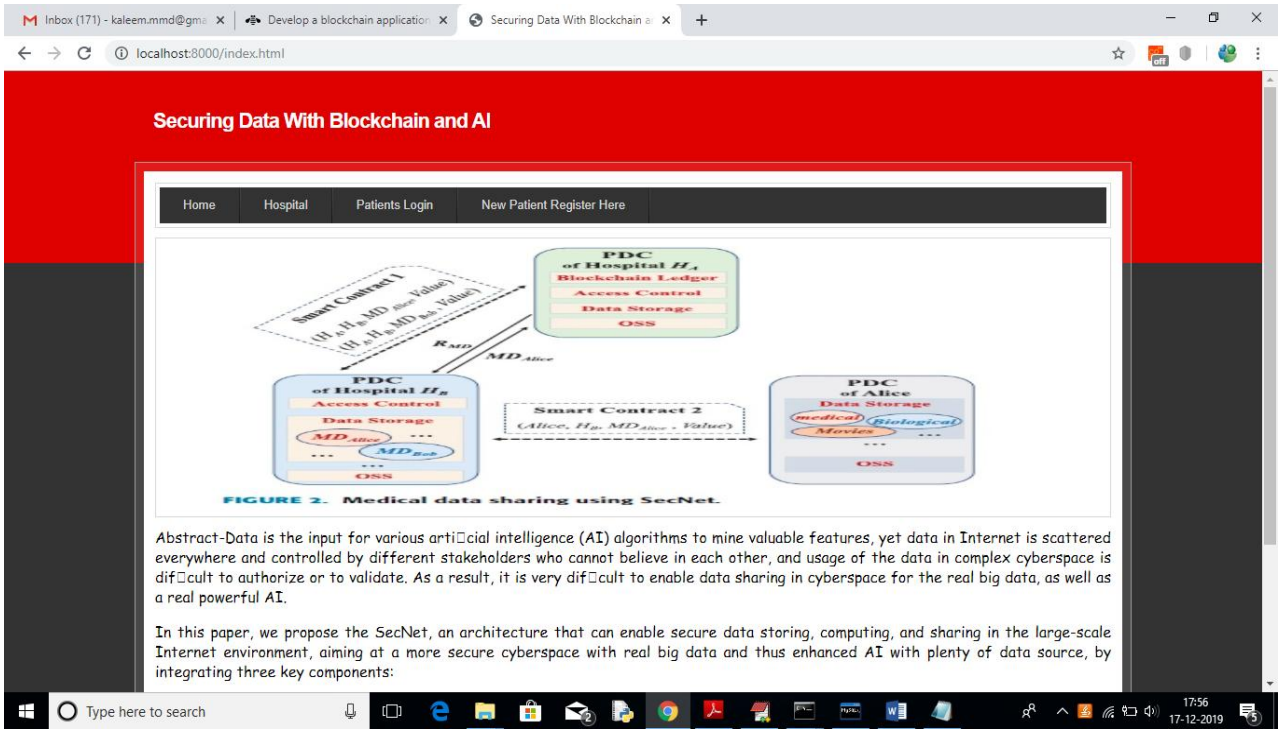
Advantages:
- Provides more data security compared to previous system.
- User will have control over his data.
- Accessing the data is difficult for user who don't have permission.

5. Implementation

In this project we taken medical data as an example for data sharing

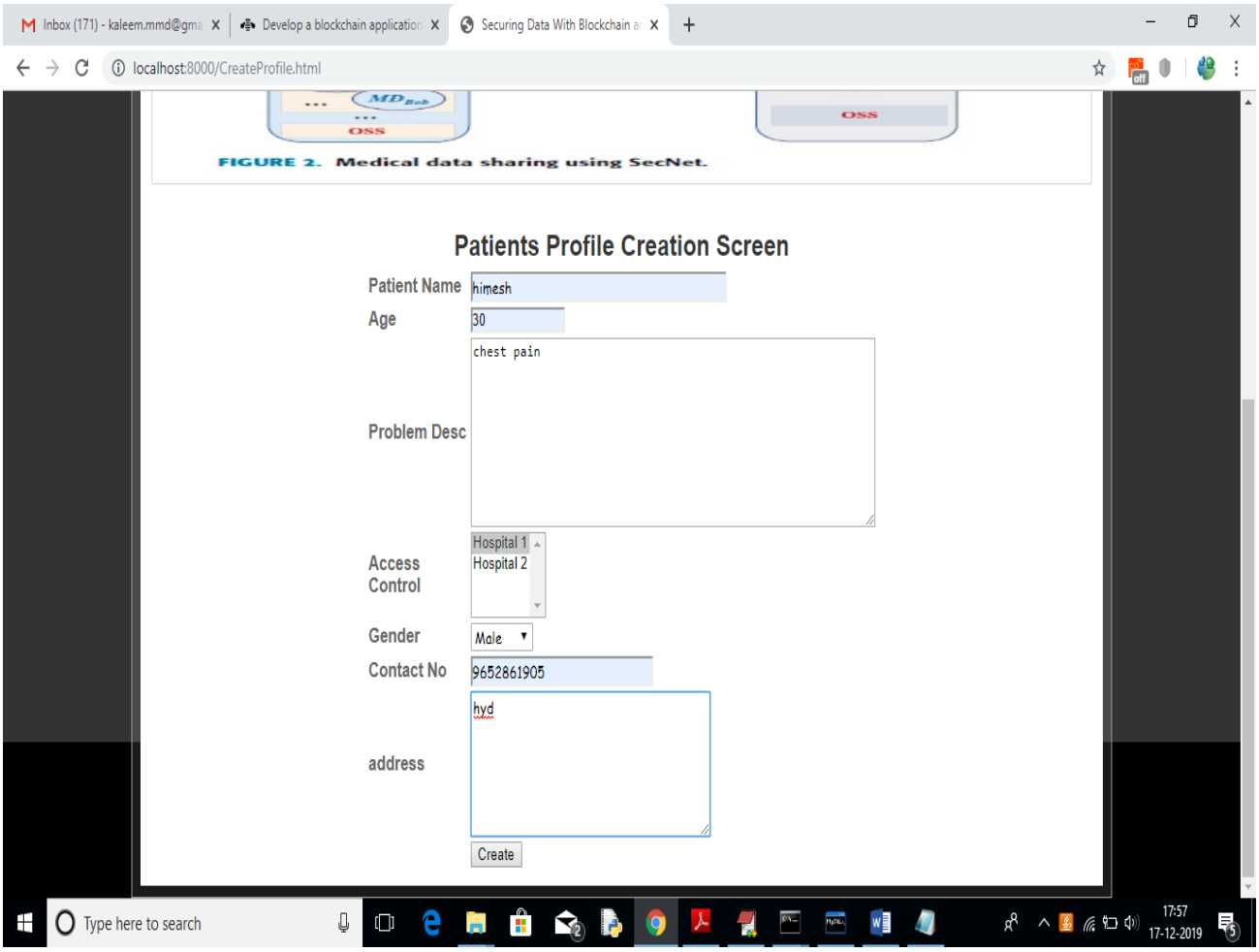
This project consists of two modules.
1) Patients and hospitals
2) Patients will create his profile with all disease details and then he give permission to the desired hospital with whom he wish to share his details while creating his profile blockchain object will be created with allowable permissions and it will allow only those hospital to access the data. There are different types of hospitals with whom patient can share data
   blockchain = Blockchain ()

6. Results

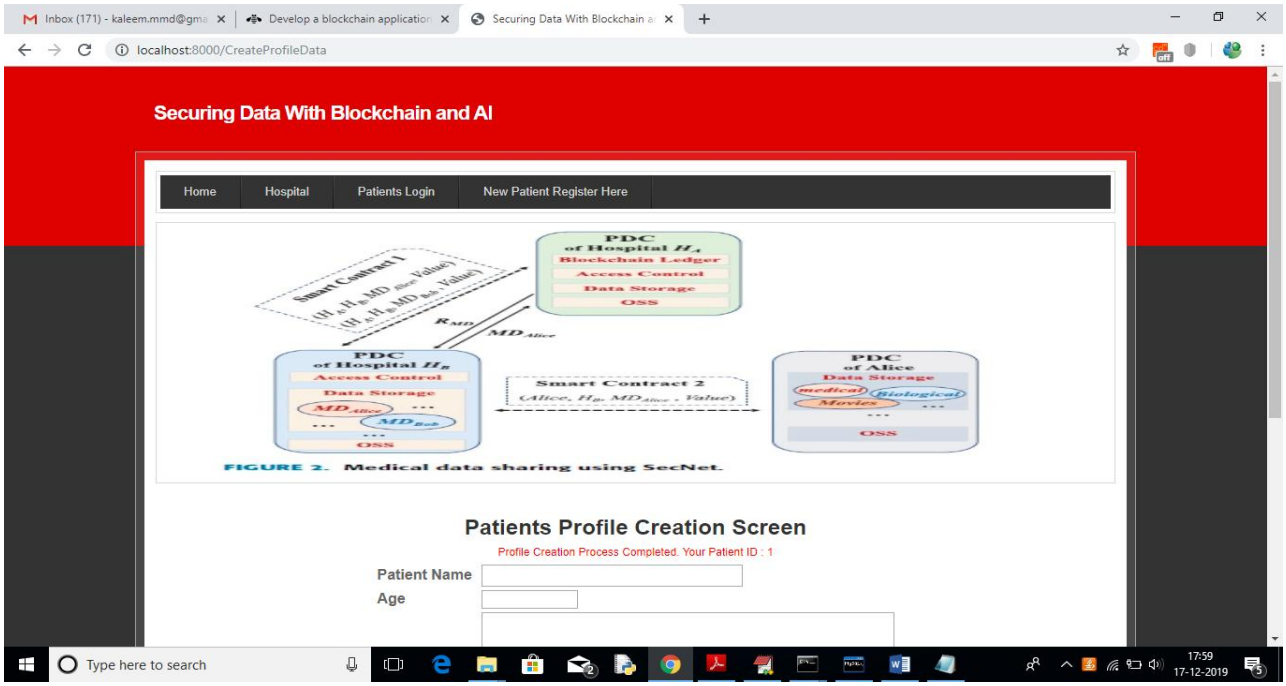


Home Screen

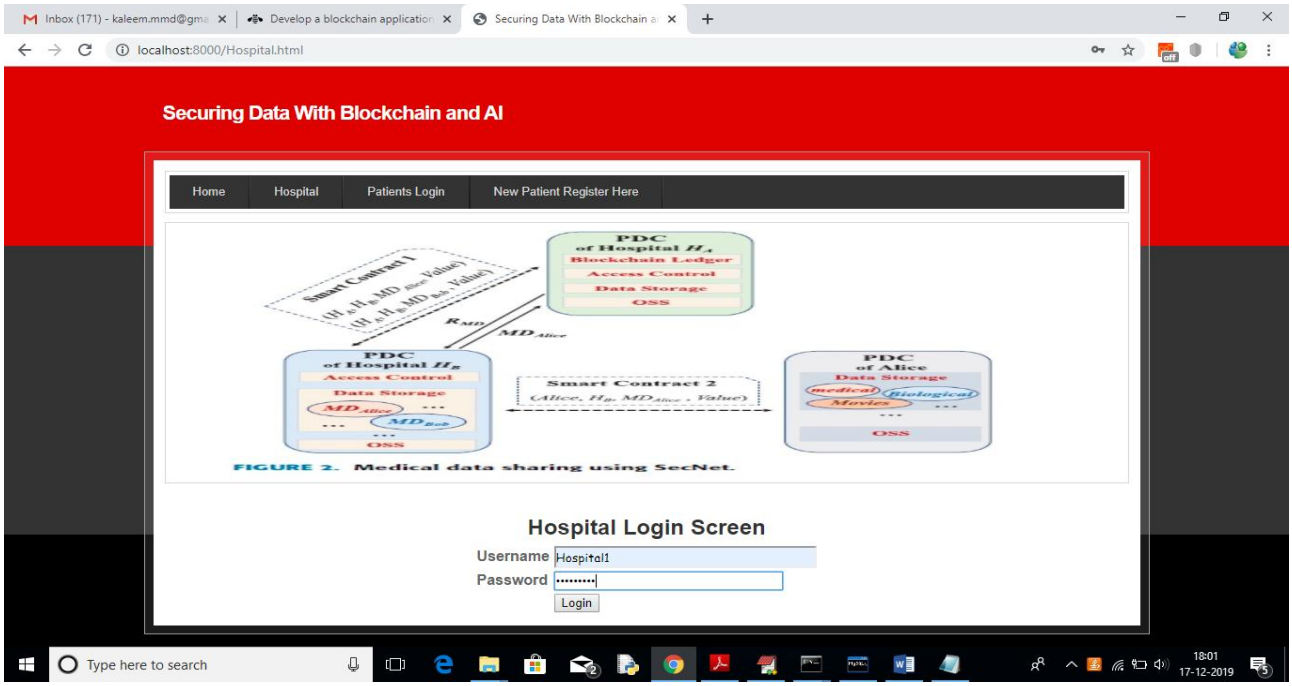
In above screen click on 'New Patient Register Here' link to get below screen



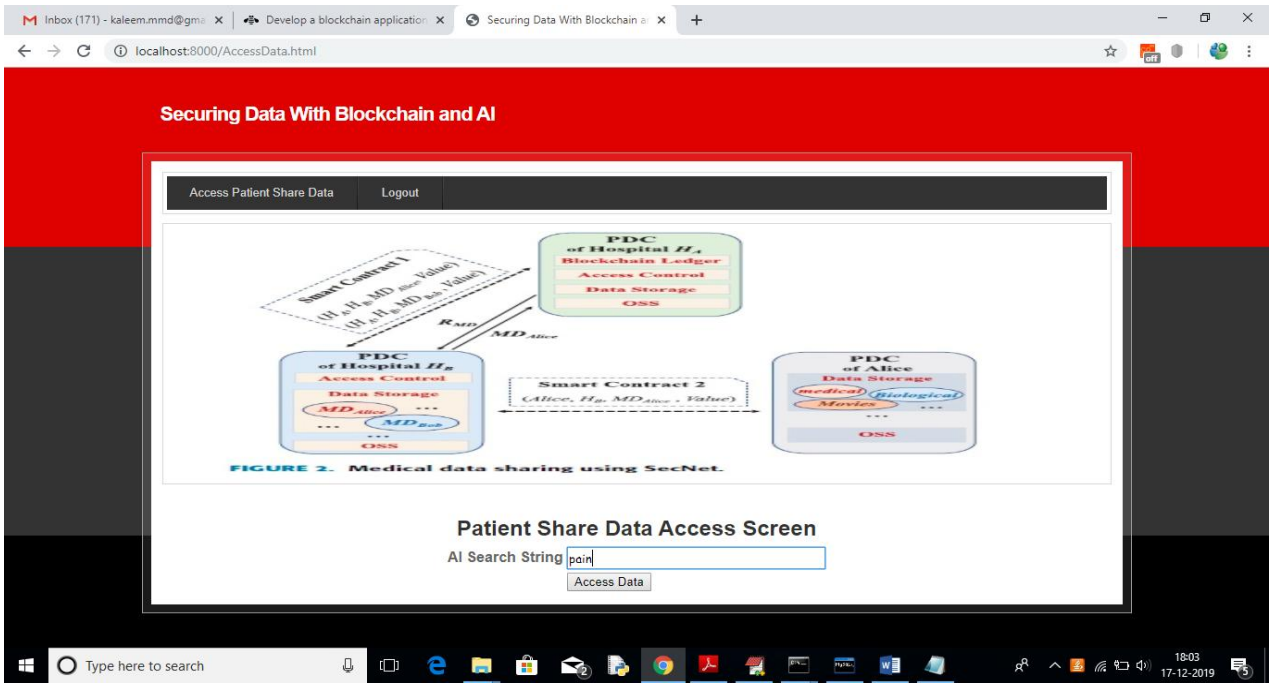
Patient enters his/her details



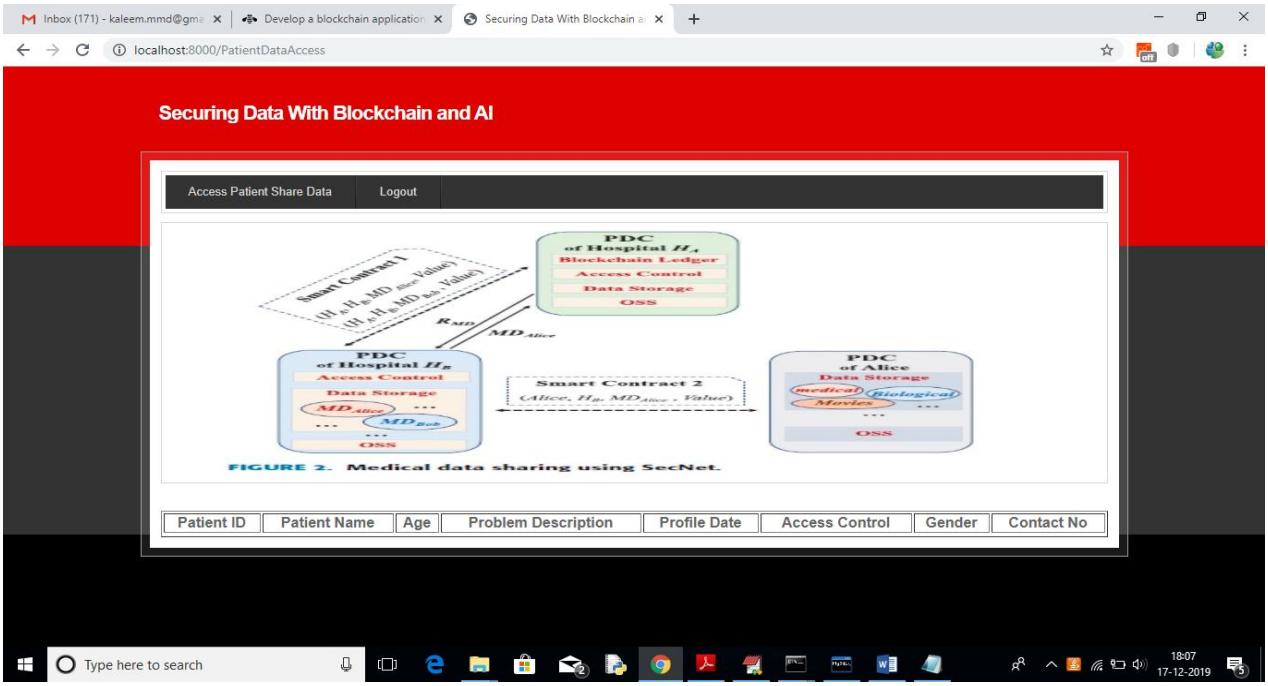
Patient Profile Creation Screen



Hospital Login Screen

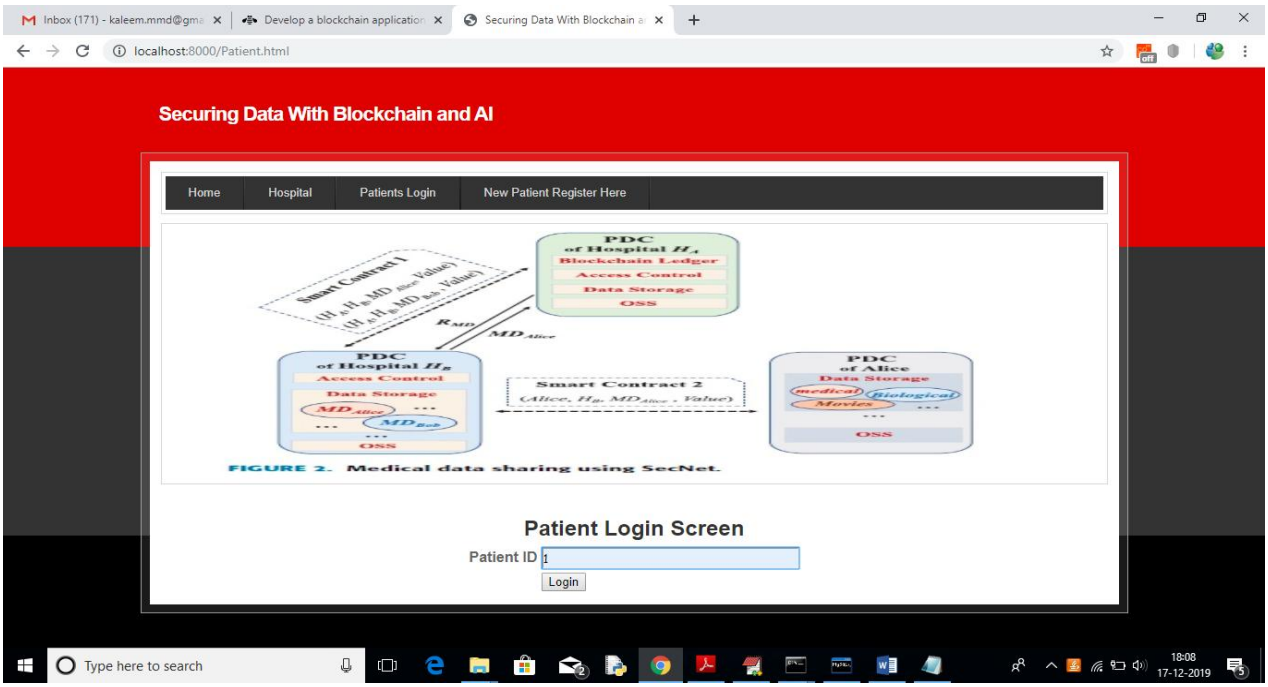


Accessing Data from Patient

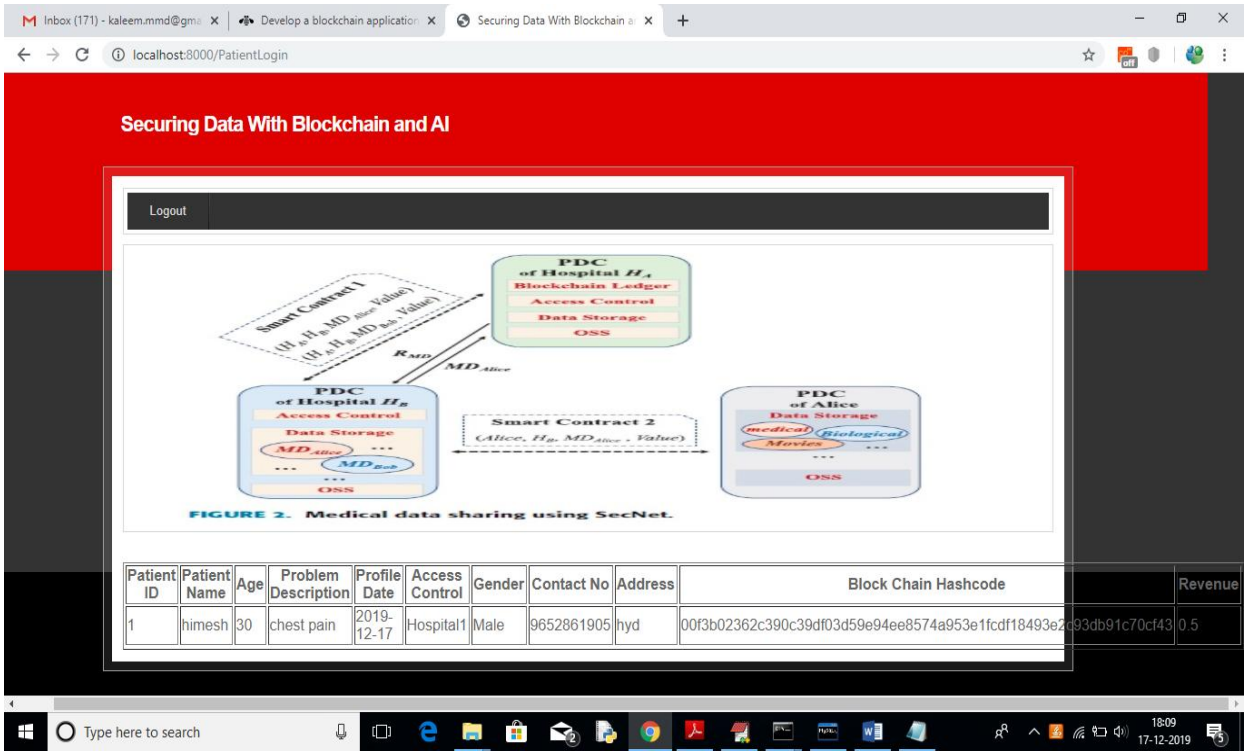


Patient Details

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



Patient Login Screen



Patient Details and hash code

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.

7. Conclusion

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.

8. Future Scope

- In future work, we will explore how to leverage blockchain for the access authorization on data requests.
- Design secure and detailed smart contracts for data sharing and AI - based computing service in SecNet.

We will model SecNet and analyze its performance through extensive experiments based on advanced platforms.

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