PERSONALIZED FEDERATED LEARNING FOR IN-HOSPITAL MORTALITY PREDICTION OF MULTI-CENTERED ICU

K. Rambabu [1], B. Anusha,

[1]**Assistant professor(HOD), P.G DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andhara Pradesh**
Email:- kattarambabudnr@gmail.com
[2]**PG Student of MCA,** Dantuluri Narayana Raju College**, Bhimavaram, Andhara Pradesh**
Email:- anushabollavarapu35@gmail.com

ABSTRACT

Federated learning (FL), as a paradigm for addressing challenges of machine learning (ML) to be applied in private distributed data provides a novel and promising scheme to promote ML in multiple independently distributed health care institutions. However, the non-ID and unbalanced nature of the data distribution can decrease its performance, even resulting in the institutions losing motivation to participate in its training. This paper explored the problem with an in-hospital mortality prediction task under an actual multi-user ICU electronic health record database that preserves the original non-ID and unbalanced data distribution. It first analyzed the reason for the performance degradation of baseline FL under this data scenario, and then proposed a personalized FL (PFL) approach named POLA to tackle the problem. POLA is a personalized one-shot and two-step FL method capable of generating high-performance personalized models for each independent participant. The proposed method, POLA was compared with two other PFL methods in experiments, and the results indicate that it not only effectively improves the prediction performance of FL but also significantly reduces the communication rounds. Moreover, its generality and extensible also make it potential to be extended to other similar cross-silo FL application scenarios.

1 INTRODUCTION

With the promotion of electronic health record (EHR) systems, a huge amount of EHR data have emerged [1]. The EHR datasets, which contain exhaustive information such as patient diagnosis and treatment, underpin the application of machine learning (ML) in digital health. Moreover, its rich resources and valuable implicit information have also made ML one of the hottest technologies in its secondary analysis [2]. Nevertheless, due to the privacy and sensitivity of EHR, the application of traditional ML which refers to centralizing or releasing these data, poses not only legal, ethical, and regulatory challenges, but also technical ones [3]. Though there are some corresponding solutions to get around these restrictions, such as removing some key information to anonymize the patient data or adding privacy-preserving algorithms in the transmission process to prevent data leakage [4], the above problem has not been fundamentally solved because they still involve data migration.

Literature Survey

Hyper connected 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 system, the loss of control overuse data has become a very serious challenge, making it difficult to protect privacy, boost innovation, and guarantee data sovereignty. In this article, we propose Hyper-Net, a novel decentralized trusted computing and networking paradigm, to meet the challenge of loss of control over data. Hyper-Net 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 block chain as well as smart contract; and the UDI platform, enabling secure digital object management and an identifier-driven routing mechanism. Hyper-Net 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.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

In cyber world everything is depend on data and all Artificial intelligence algorithms discover knowledge from past data only, for example in online shopping application user 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 reeducation 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.

Disadvantages:

An existing system utilized a heuristic algorithm involving automated machine learning (Autumn) in the optimization of personalized models, which may be confused with existing comparable studies.

Proposed System & alogirtham

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

Blockchain: Blockchain-based data sharing with owner's hip guarantee, which enable strutted 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 shared and give permission.

4.1 Advantages:

The proposed scheme is a two-step and one-shot PFL, the overview of which is illustrated in the step here refers to FL training and local adaptation, where FL training is to obtain a shared model with adequate global generalization experiment, and local adaptation is a subsequent step to generate high-performance personalized models for independent individuals.

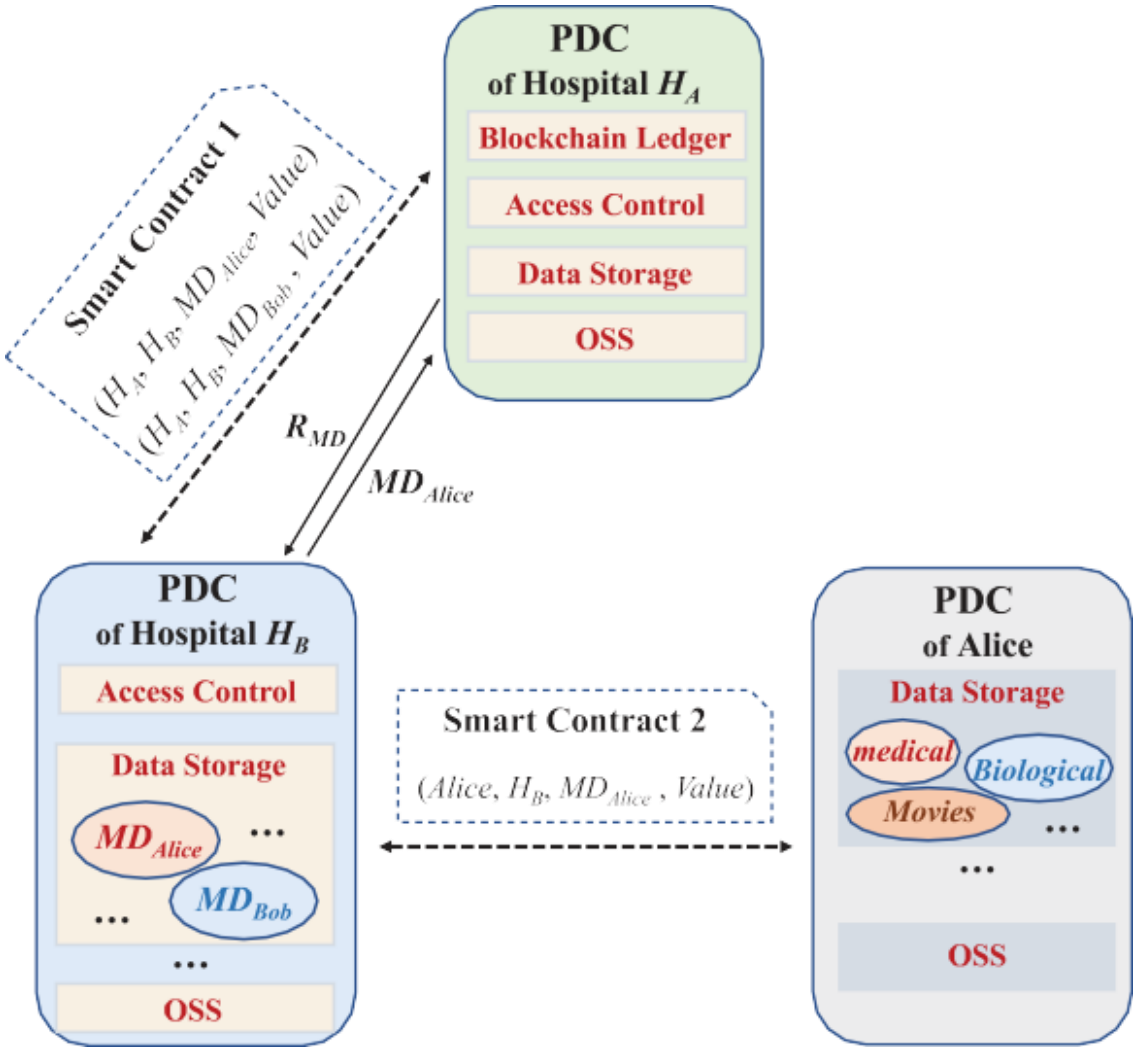


Fig:3.1 System Architecture

IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such a Browse Hospital Datasets and Train & Test Data Sets, View Trained and Tested Hospital Datasets Accuracy in Bar Chart, View Trained and Tested Hospital Datasets Accuracy Results, View Prediction of Hospital Mortality Prediction, View Hospital Mortality Prediction Ratio, Download Morality Predicted Data Sets, View Hospital Mortality Prediction Ratio Results, View All Remote Users.

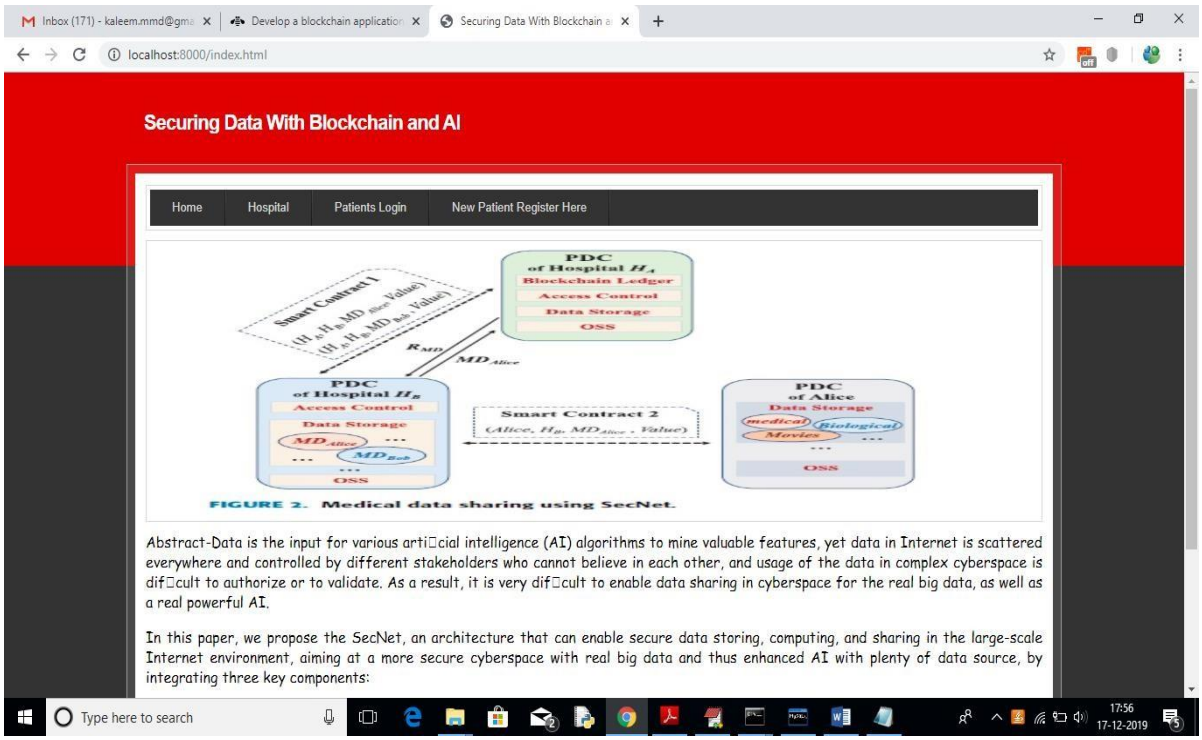
5 RESULTS AND DISCUSSION

SCREENSHOTS

HOME SCREEN

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. pie' file alsochangeportnoto3306

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

Fig.1.Securing data with blockchain

CREATE NEW PATIENT REGISTRATION

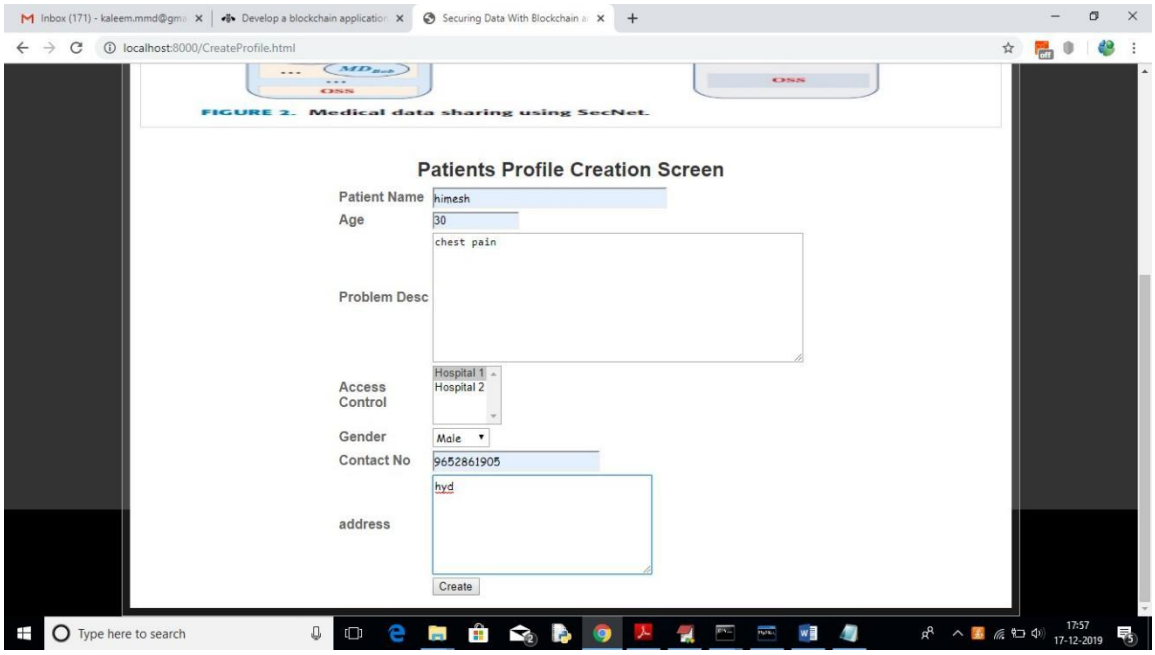


Fig.2.Patients profile creation screen

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

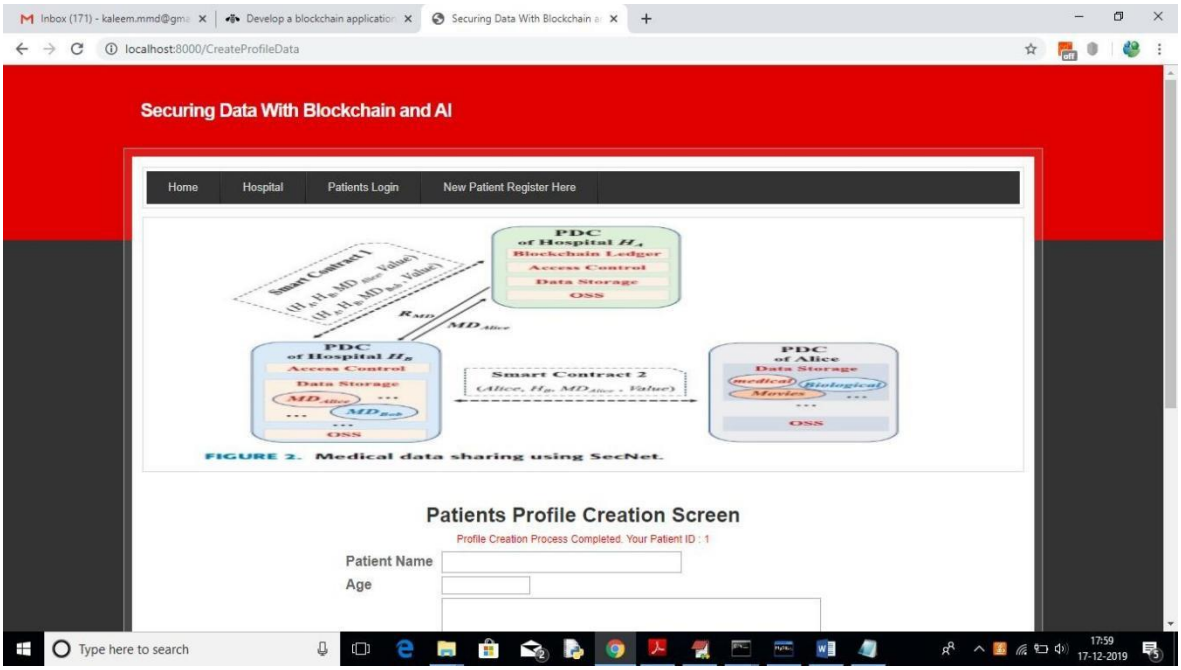


Fig.3.Patiatent profile

In above screen one patient is created with patient ID1andnowHospital1 can login and search and access this patient data as patient has given permission to Hospital1

HOPITAL LOGIN SCREEN

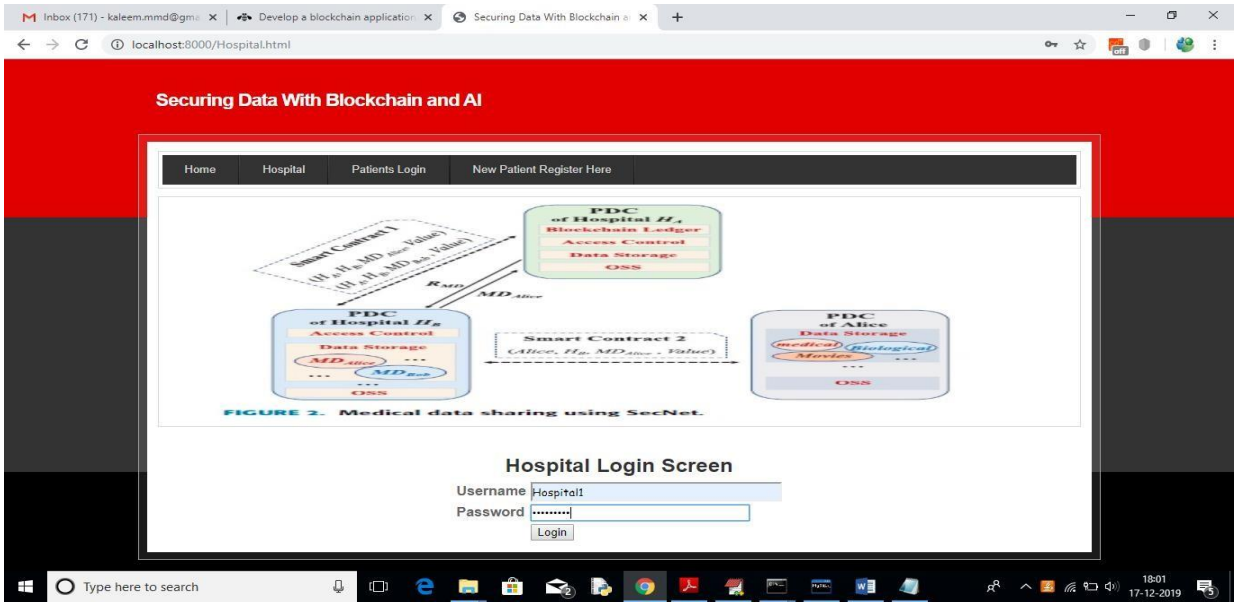


Fig.4.Hospital login screen

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 Hospital2tologin as Hospital2. After login will get below screen

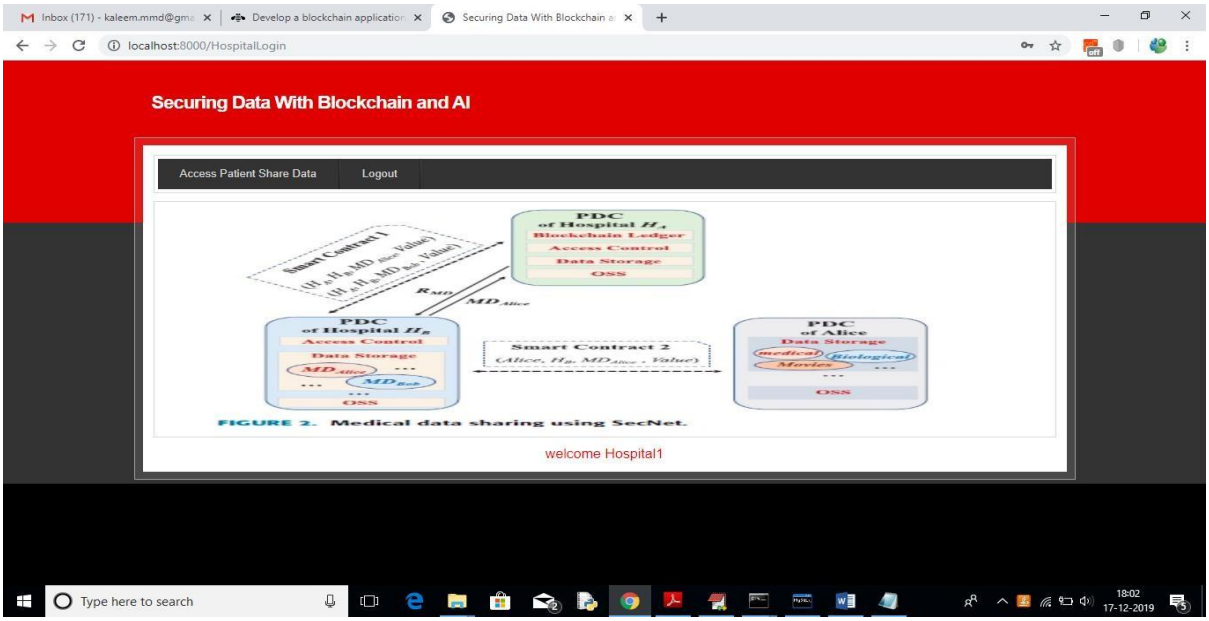


Fig.5. Security data

ACCESSPATIENTSHAREDATASCREEN

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

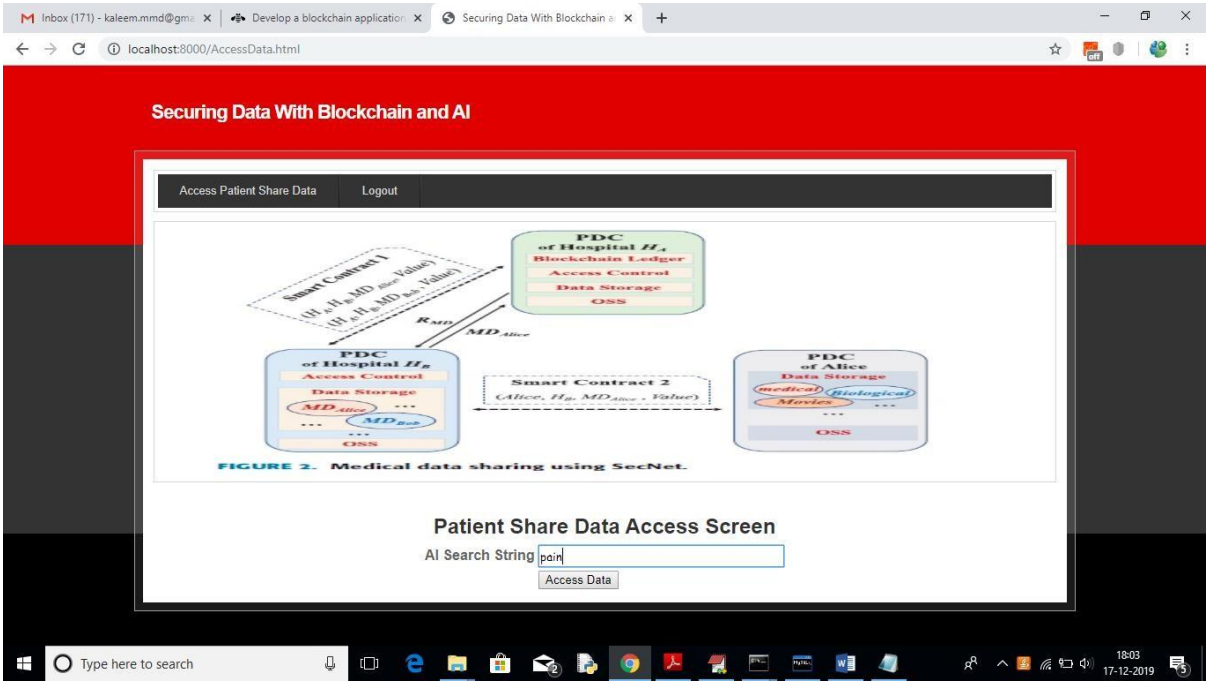


Fig.6. Patient share data access screen

In above screen I want to search for all patient who are suffering from 'pain' and then click on 'Accessdata' button to get below screen.

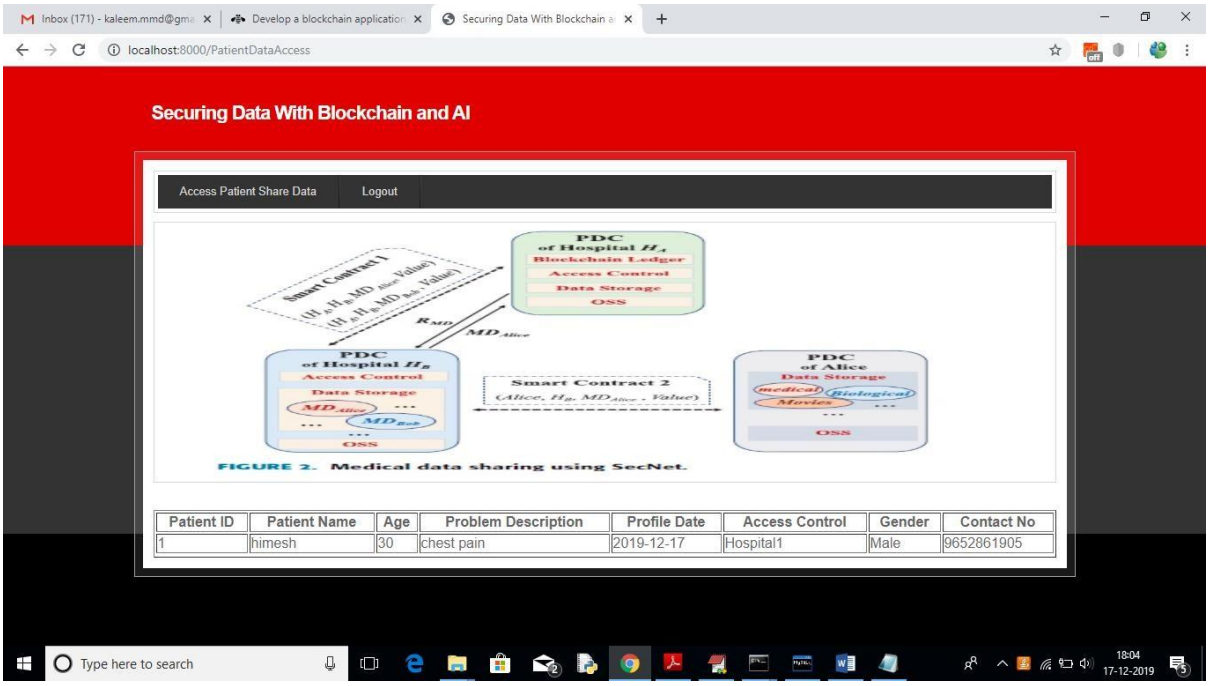


Fig.7. Securing data

In above screen Hospital1getting details of patient and Hospital2 not having permission so it will not get details. To see this logout and login as Hospital2.

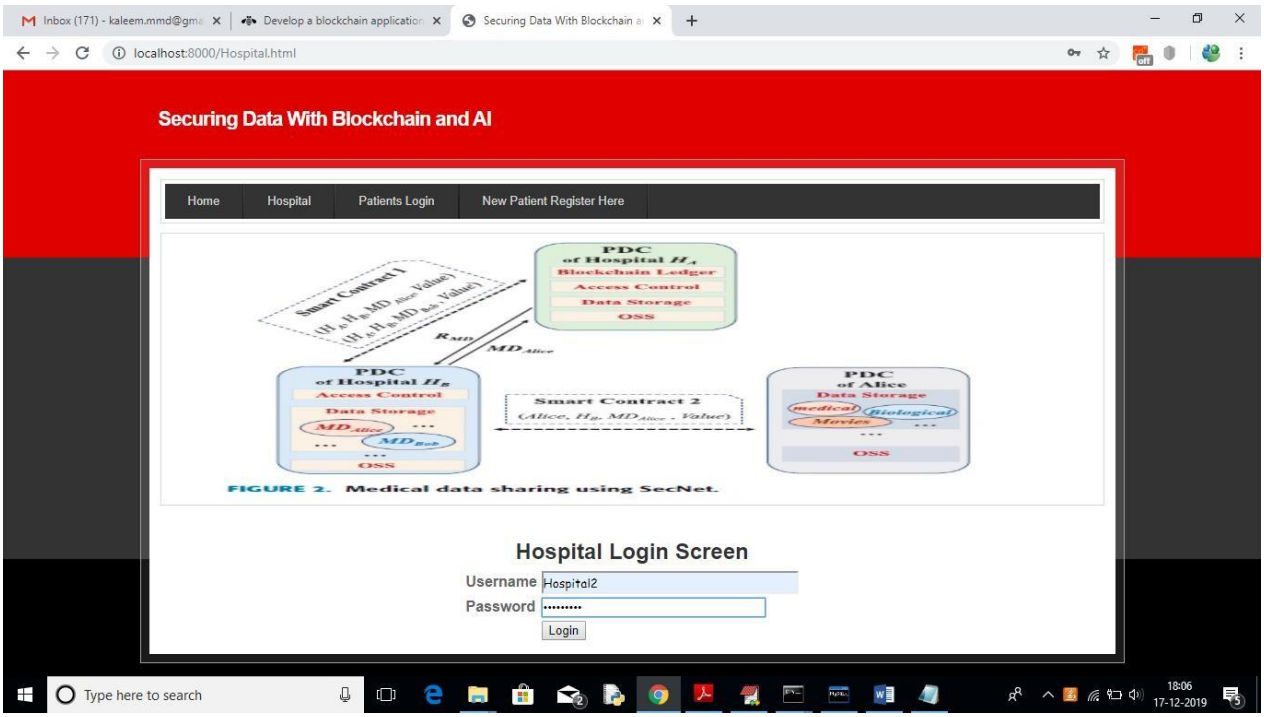


Fig.8. Hospital login

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

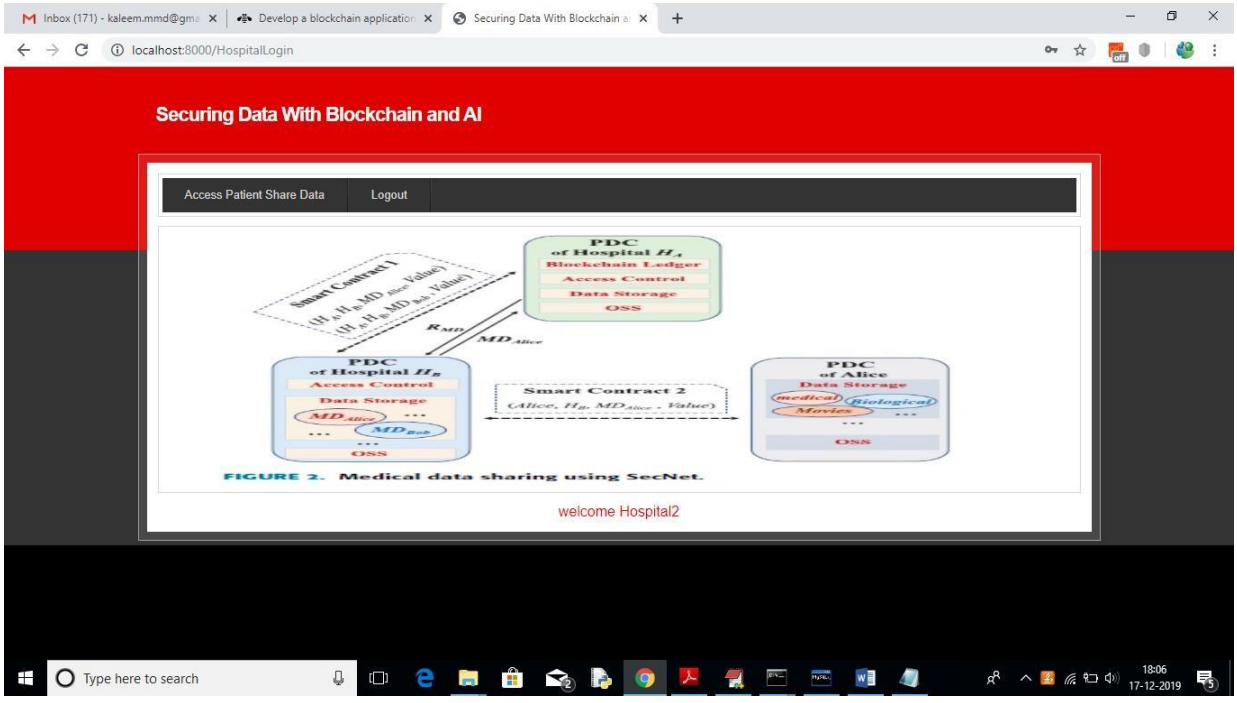


Fig.9. Securing data

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

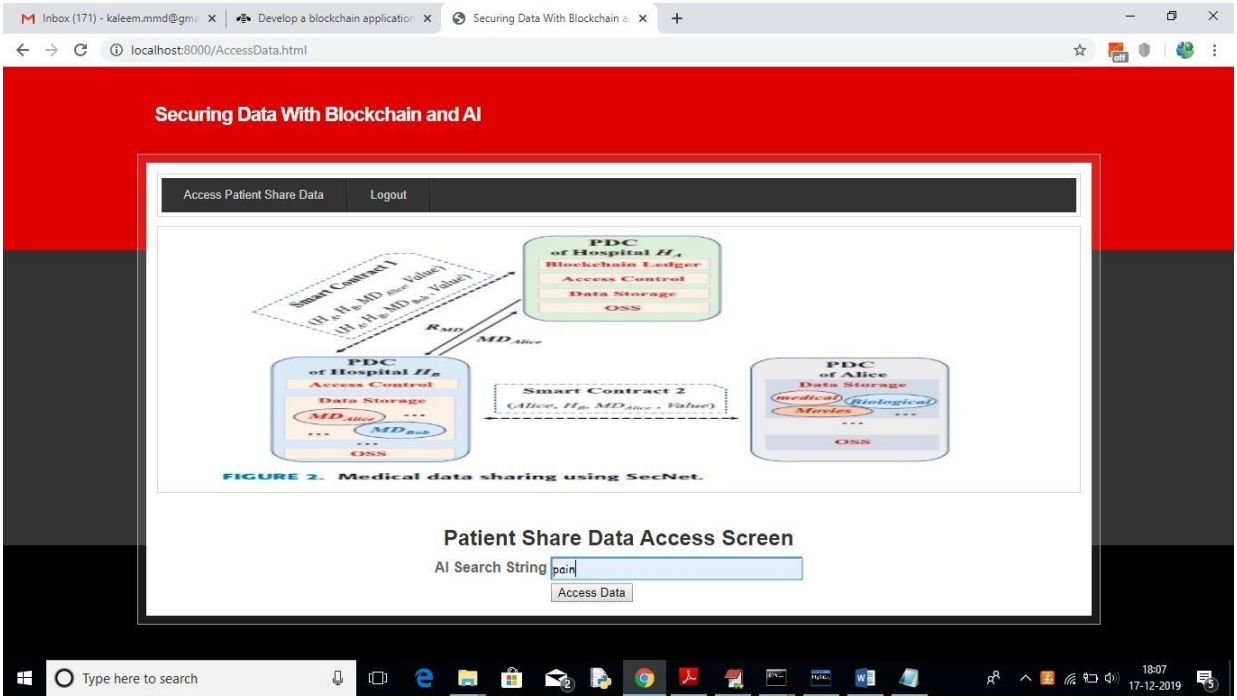


Fig.10. Access screen

For above query will get below result

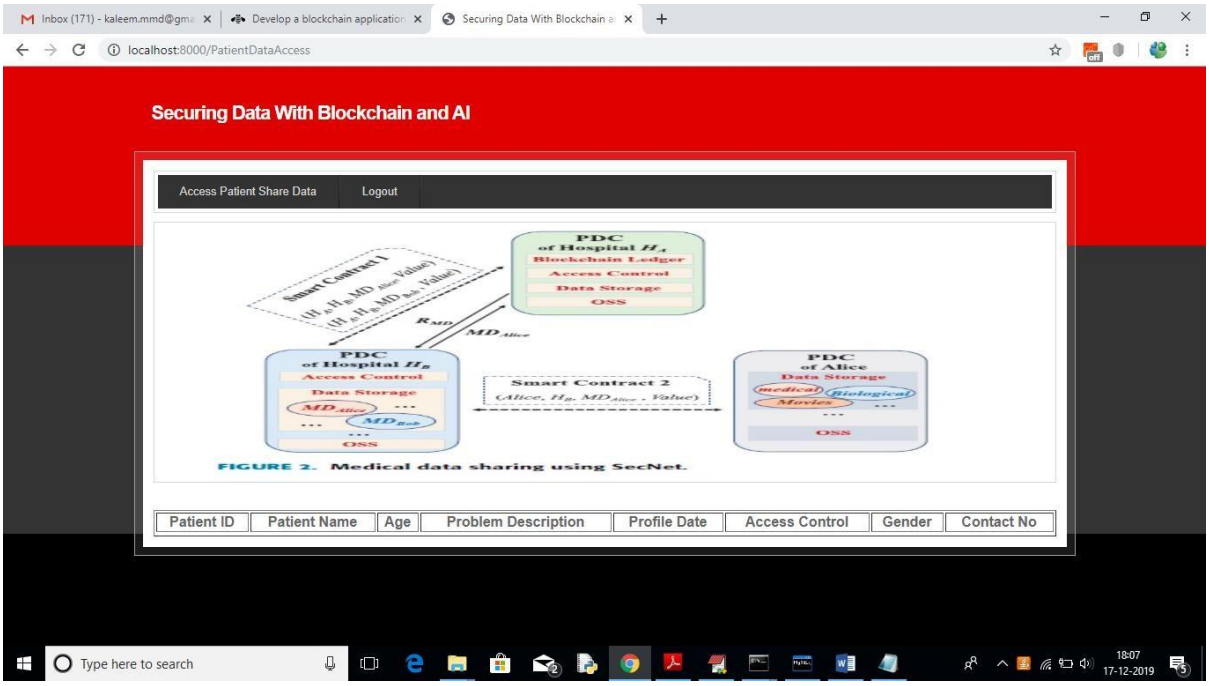


Fig.11.Block chain

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

PATIENT LOGIN SCREEN

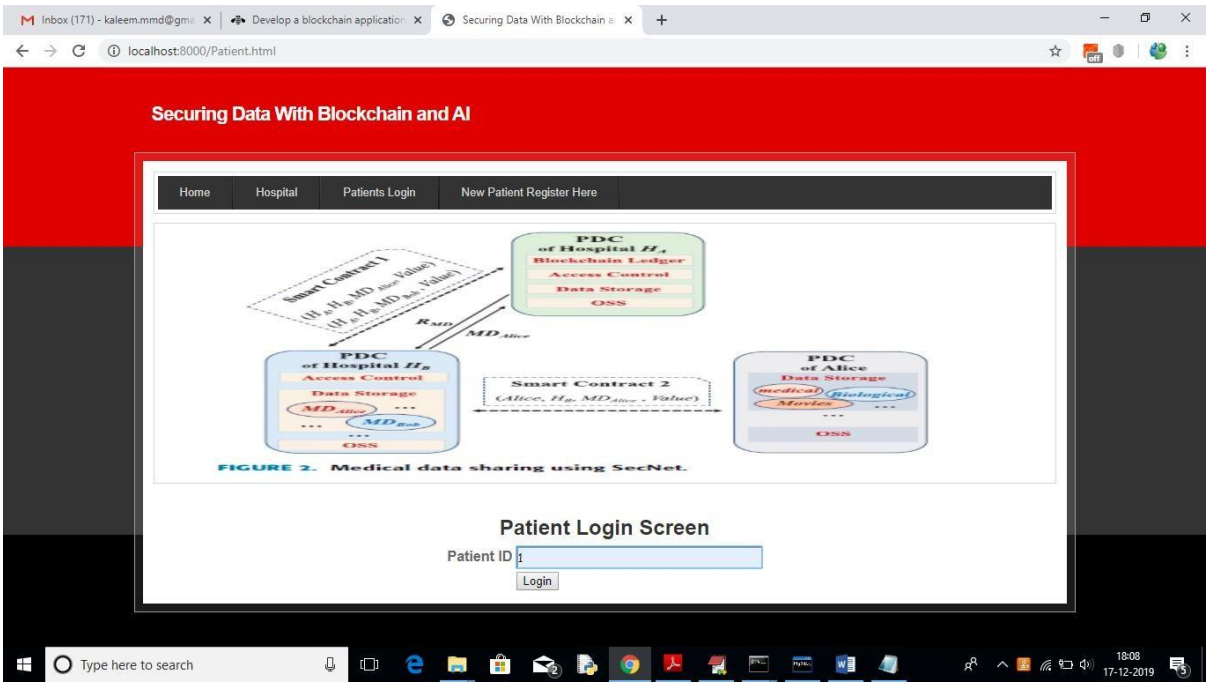


Fig.12. Patient login

After login will get below details forpatient1

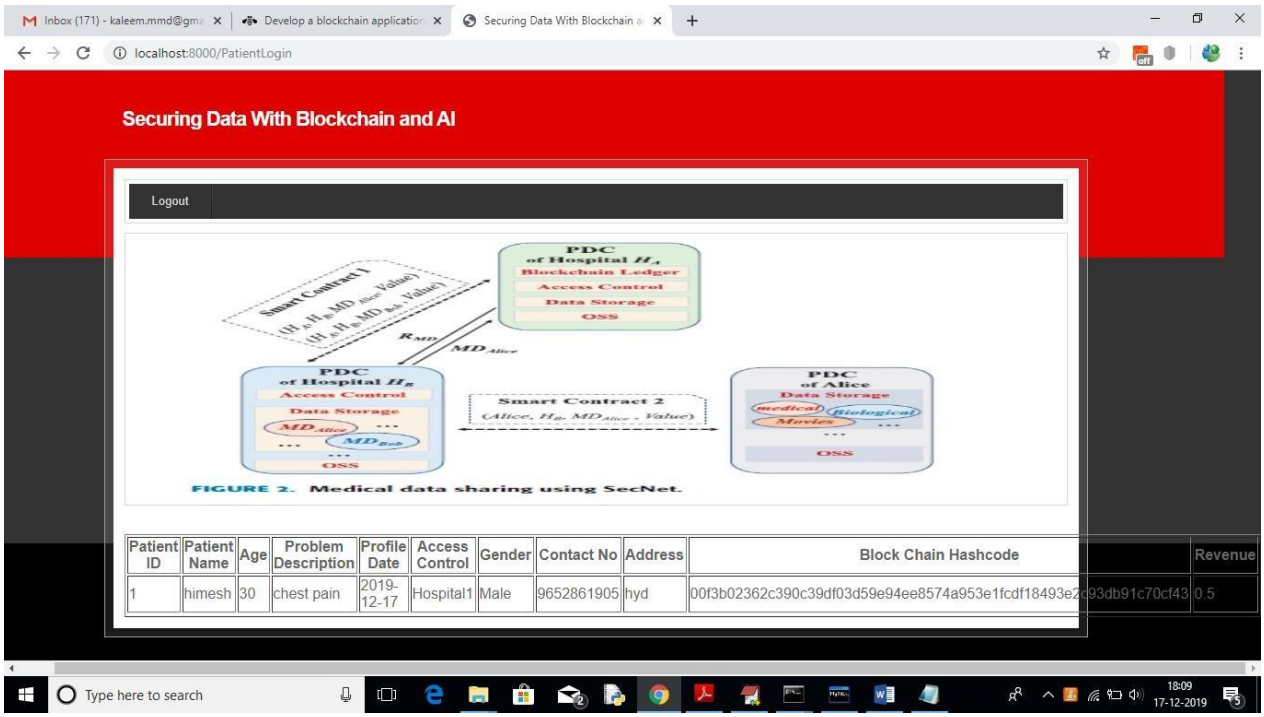


Fig.13. Securing data

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.

6. CONCLUSION AND FUTURE WORK

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 Sec-net, Which Is a New Networking Paradigm Focusing on Secure Data Storing, Sharing and Computing Instead of Communicating. Sec-net Provides Data Ownership Guaranteeing with The Help of Block chain Tech-Neologies, 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 Sec-net In Medical Care System, And Gives Alternative Ways for Employing the Storage Function of Senet. Furthermore, We Evaluate Its Improvement on Network Vulnerability When Countering Dods Attacks, And Analyses the Inventive Aspect on Encouraging Users to Share Security Rules for A More Secure Network.

7. REFRENCES

H. Yin, D. Guo, Kwang, Z. Jiang, Y. Lyu, and J. Xing, ``Hyperconnected network: A decentralized trusted computing and networking paradigm," IEEE Net., vol. 32, no. 1, pp.112117, Jan./Feb. 2018.

K. Fan, W. Jiang, H. Li, and Y. Yang, ``Lightweight RFID protocol for medical privacyprotectioninIoT," IEEE TransInd.Informant., vol. 14, no.4, pp.16561665, Apr. 2018.

T. Chafed, J. Genet, J. Van Den Hoof, M. F. Kaashoek, J. Mickens, R. Morris, and N. Nedovic, ``Amber: Decoupling user data from Web applications, "in Proc.15thWorkshopHotTopicsOper. Syst. (Hoot's XV), Warth-Wein Ingen, Switzerland,2015, pp.16.

Molecule, R. Spahn, R. Gambas, T.-K. Huang, ands. Sen, ``Enhancing selectivity in bigdata," Biosecurity Privacy, vol. 16, no. 1, pp. 3442, Jan./Feb.2018.

Y.-A. de Montoya, E. Shmueli, S. Swing, and A. S. Pentland, ``opens: Protecting the privacy of meta data through Safe Answers, " Plops ONE, vol.9, no. 7,2014, Art.no. e98790.

C. Perera, R. Ranjan, and Laing, ``End-to-end privacy for open big data markets," IEEE Cloud Compute., vol. 2, no. 4, pp. 4453, Apr. 2015.

X. Zheng, Z. Cai, and Y. Li, ``Data linkage in smart Internet of Things systems: A consideration from a privacy perspective, "IEEE Common. Mag., vol.56, no.9, pp.5561, Sep.2018.

Q. Land, ``Adaptable block chain-based systems: A case study for product traceability, 'Geosoft., vol.34, no. 6, pp.2127, Nov./Dec.2017.

Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, ``Deep learning-based inference of private information using embedded sensors in smart devices "Veenema., vol.32, no.4, pp.814, Jul./Aug. 2018.