Journal of Advanced Zoology

ISSN: 0253-7214

*Volume **45 Special** Issue **02 Year 2023** Page **1396:1405***

Securing Healthcare: A Fusion of AI and Blockchain for Medical Data Protection

Dr. Rugada Vaikunta Rao[#1], Mrs. A.Laxmi Prasanna [#2], Mr. Gugloth Ganesh [#3], Mrs.Vadla Anuja [#4],Mr.Konatala Lokesh[#5] , Dr.K.Vasanth Kumar[#6]

[#1]Professor, Department of Civil Engineering
Dadi Institute of Engineering and Technology, Anakapalle,
[#2] Assistant Professor, Department of Computer Science and Engineering,
Malla Reddy Engineering College(A),Hyderabad,Telangana-500100.
[#3]Assistant Professor, Department of Computer Science and Engineering,
Malla Reddy Engineering College(A),Hyderabad,Telangana-500100.
[#4]Assistant Professor, Department of Computer Science and Engineering(IoT),
Malla Reddy Engineering College (A), Hyderabad,Telangana-500100.
[#5]Assistant Professor, Department of Computer Science and Engineering,
Malla Reddy Engineering College (A), Hyderabad,Telangana-500100.
[#6]Professor, Department of Computer Science and Engineering,
Malla Reddy Engineering College (A), Hyderabad,Telangana-500100.

Corresponding Email ids: Vrugada@gmail.com [1] , prasannababli@gmail.com [2] , nayakganesh171@gmail.com [3] , anujavadla@gmail.com [4], lokeshnist@gmail.com [5], vasanthkamatham@gmail.com [6],

Article History
Received: 11 March 2023
Revised: 21 August 2023
Accepted: 03 October 2023

ABSTRACT

Today's digital environment places a high value on data, which includes intellectual property, private consumer information, and long-term corporate strategies. It is crucial to protect this priceless asset from the suspicious eyes of hackers. A complete strategy must be used to address the six major areas of governance, discovery, protection, compliance, detection, and reaction in order to accomplish comprehensive data security. The foundation for data security is laid by governance first and foremost, which calls for the creation of strong policies, data classification processes, an exhaustive list of all available data assets, and a sturdy infrastructure. The next crucial step in guaranteeing data safety is to identify the data's sources, whether they be databases, files, or network systems. Encryption, diligent key management, strict access control measures, and trustworthy data backup procedures must all be put into place in order to protect data efficiently from unauthorized access or breaches. A crucial aspect of compliance is the creation of accurate reports and the preservation of crucial documents. However, the modern cyberspace is a complicated maze of dispersed data, controlled by unrelated organizations lacking in mutual trust. It is difficult to enable safe data sharing and authentication over the internet due to this complex environment, especially when working with massive amounts of data and artificial intelligence systems. The combination of blockchain technology and artificial intelligence (AI) presents a strong solution to this problem. The effectiveness of using AI and blockchain to strengthen the security of medical data is examined in this article. We want to give end users a secure environment by utilizing these cutting-edge technologies, protecting the integrity and security of private medical data in a society that is becoming more linked.

KEY WORDS: Block Chain, Artificial Intelligence, E-Governance, Data Management, Distributed Systems, Hackers, Medical Data.

1. INTRODUCTION

In Development of cyber security by increasing of CPS in the entire globe makes the life of the people easy to interact with the outside of a globe. Data of the user becomes very crucial. This data of a user is the property of the owner. The owner having full control of data belongs to the owner itself. But hidden sensors of the technology can reveal the private data of the owner by the companies to meet the competitiveness. The information about the customer location, customer activities of browsing data, calls made by customer, customer preferences, are gathered by companies without the prior knowledge of the customer. This is the problem of privacy preservation of the individual.

Because of the untrusted environment between the stake holders customers will not give complete data to share by the internet. So this data given by customers are not enough for AI to train and analyze. By the development of Block chain technology gives hope to solve this problem for privacy preservation. With block chain technology and AI are more useful to collect big data from different sources of internet can give best and accurate results. SecNet influences the current Blockchain concept in-order to avoid the misuse of data. The SecNet also provide trust even in the environment which is untrusted

The prime objective of this work is to provide data safety and confidentiality of the user. Here the combination of AI and Block chain forms secure architecture called SecNet for the optimality of security while data is to be shared and also the security of the network where data is travelling. Customers give their data to the CSP for applications and service uses. SecNet have the responsibility to store data in a protected way. Development of cyber security by increasing of CPS in the entire globe makes the life of the people easy to interact with the outside of a globe. Data of the user becomes very crucial. This data of a user is the property of the owner. The owner having full control of data belongs to the owner itself. But hidden sensors of the technology can reveal the private data of the owner by the companies to meet the competitiveness. The information about the customer location, customer activities of browsing data, calls made by customer, customer preferences, are gathered by companies without the prior knowledge of the customer. This is the problem of privacy preservation of the individual.

2. LITERATURE SURVEY

This section will deal with all the previous information related to importance of block chaon and security threats which occur on the medical data . Literature survey is the most important step in software development process. For any software or application development, this step plays a very crucial role by determining the several factors like time, money, effort, lines of code and company strength. Once all these several factors are satisfied, then we need to determine which operating system and language used for developing the application. Once the programmers start building the application, they will first observe what are the pre-defined inventions that are done on same concept and then they will try to design the task in some innovated manner.

MOTIVATION

1) Enhancing Selectivity in Big Data.

Mathias Lecuyer et al. [3] discussed about the enhancing selectivity in big data how companies today collect massive volumes of personal data and make it widely available throughout the organisation. This exposes the data to external hackers and employees who violate their privacy. This study demonstrates that, for a diverse and critical set of workloads, only a portion of the data is required to achieve state-of-the-art accuracy. We propose selective data systems that are intended to identify the data that is important for a company's present and evolving workloads. These technologies limit the availability of data by separating out information that isn't genuinely valuable.

2) Pyramid: Enhancing Selectivity in Big Data Protection with Count Featurization

Mathias Lecuyer et al. [4] discussed that importance of enhance selectivity in pyramid model by protecting massive amounts of data is a formidable task for the expanding number of organisations who gather, store, and monetize it. The capacity to discriminate between data that is genuinely required and data acquired "just in case" would assist these organisations in limiting the latter's vulnerability to attack. A natural strategy would be to monitor data consumption and preserve only the working-set of in-use data in accessible storage, while unused material is evicted to a highly secure repository. However, many of today's big data applications rely on machine learning (ML) workloads that are retrained on a regular basis by accessing and thus exposing the entire data store to attack.

3) Adaptable Blockchain-Based Systems: A Case Study for Product Traceability.

Qinghua Lu et al. [5] adopted the block chain based system for product traceability. Tracing the provenance of items across complicated supply chains necessitates a transparent, tamper-proof metadata infrastructure that is both trusted by all parties involved and adaptive to changing environments and regulations. Can such sophisticated infrastructure be implemented decentralizedly? Qinghua Lu and Xiwei Xu tell the story of how they created the originChain system, which uses new blockchain technology.

4) Artificial intelligence and big data

D. E. O’Leary et al. [6] discussed the importance of AI and big data as AI Innovation in Industry is a new department for IEEE Intelligent Systems, and this paper examines some of the fundamental concerns and applications of AI for big data (AI has been used in a variety of ways to aid in the capture and structuring of big data, as well as to analyse big data for key insights).

3. EXISTING METHODOLOGY

For patient privacy and data security, it is essential to protect sensitive medical information. Medical records used to frequently be kept in physical files, which left them open to unwanted access. Today, there are a number of techniques and technologies available to improve the security of medical data, thanks to the digitization of healthcare data and the usage of cloud servers:

LIMITATION OF EXISTING SYSTEM

1. Human mistake: Human mistake continues to be a major contributor to privacy violations and data breaches. Employees or healthcare professionals may unintentionally handle patient

data incorrectly, such as by transmitting private information to the incorrect person or falling into phishing scams.

2. Insider Threats: Despite access controls, insider threats are a constant concern. Authorized individuals with access to medical records may inadvertently or willfully abuse their privileges, resulting in data breaches.
3. Healthcare systems frequently rely on a variety of software and EHR systems, some of which may not be completely interoperable. This may make it difficult to securely share and access patient data on several platforms.
4. Cyberattacks: Due to the high value of medical data, the healthcare industry is a top target for cyberattacks. Cybercriminals may employ complex methods to get past security barriers and steal critical data.
5. Resource Limitations: Smaller healthcare companies might not have enough financial and technological resources to put strong security measures in place and stay on top of evolving threats.
6. Legacy Systems: A few healthcare facilities still rely on antiquated security mechanisms that make them more susceptible to attacks.
7. Patient Control and Access: It might be difficult to balance patient control over their own medical records with privacy concerns. It might be difficult to provide patients control over their data while maintaining security.
8. Compliance with regulations: Adhering to regulations like HIPAA in the US or GDPR in Europe can be difficult and time-consuming. A failure to comply may have legal repercussions.
9. Medical data must be shared for study and for the benefit of the general public's health. Finding the ideal balance between patient privacy and data exchange can be challenging.
10. Emerging Technologies: As telemedicine, IoT devices, and wearable health monitors become more widely used in healthcare, new security issues in protecting the data produced by these technologies appear.
11. Patient Identity Verification: It might be difficult to confirm a patient's identity in digital environments and to ensure that the proper person has access to their medical records.

4. PROPOSED SYSTEM & ITS ADVANTAGES

The proposed system uses block chain technology used for data sharing in a trusted way with guaranteed proprietary ship of data and forms a big data. This technology possesses control over the data to grant permission only some data points and some data elements are preserved privately. There will be absolute data control over the big data available. Only the permitted data can be accessed by the users. In this Block chain technology owner can add, delete, share and subscribe data and can have full control on data to give permissions in restricted environment.

ADVANTAGES OF PROPOSED SYSTEM:

The following are the benefits of the proposed system. They are:

1. **Enhanced Data Security:** Blockchain technology has strong security features that make it extremely resistant to illegal access, tampering, and data breaches. By doing this, confidential medical information is kept secure.
2. **Trusted Data Sharing:** The decentralized and immutable characteristics of the blockchain promote trust among parties. Patients, healthcare professionals, and other parties with permission may share and access data with trust in its accuracy.

3. **Big Data Management:** Large-scale medical data consolidation into a single big data resource is made possible by the system's support for big data management. This may result n healthcare analytics and research that are more thorough and informative.

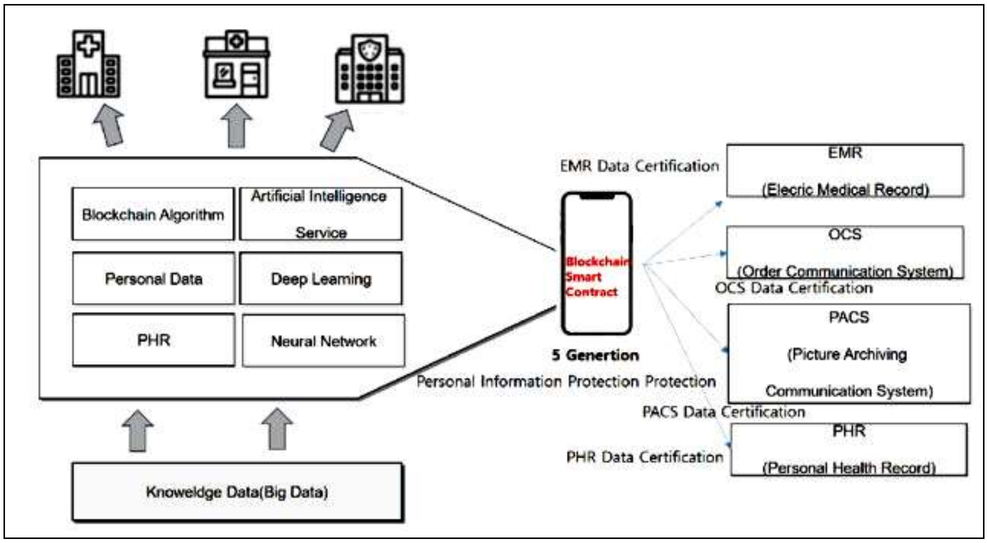

Figure 1. Denotes the Proposed Architecture

Figure 1, clearly represents the proposed architecture and it contains Patient Health Record(PHR) Storage into the cloud server using data storage and those who want to access any information ,need to have access control permission. Once the access control is present for that end user, then only he/she can able to access the file from the cloud server.

5. PROPOSED ALGORITHMS

In this proposed application we try to implement AI technique and construct a CNN model using Block Chain for Providing Security for the Medical data which is stored into the cloud server.

Proposed AI Model

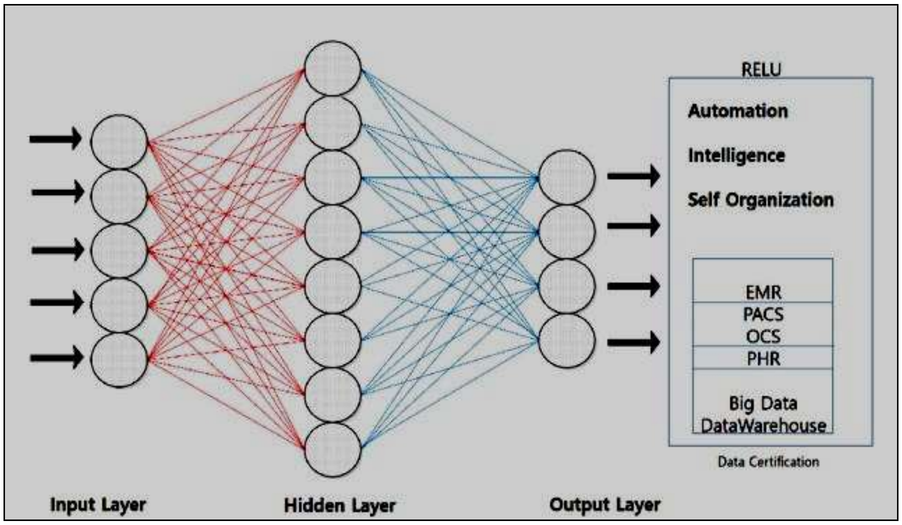

Figure 2. Denotes the Proposed CNN Model for Medical Data Security

Figure.2 clearly represents the architecture of ANN model for providing security for the medical data which is stored into the cloud server. It was one of the first CNN architectures to demonstrate excellent performance on medical data and has since become a popular benchmark for several areas. Initially the model contains three layers: Input Layer, Output Layer and Hidden Layer. The input layer takes the input from the user, here the input is nothing but patient health record which is to be processed securely into the cloud server. Now the hidden layer is one where the logic part is applied in order to make that input data secure. Here we try to use several filters to make the plain text into encrypted manner. For this we use block chain algorithm. Next we try to extract the corresponding result as output, which is nothing but secured data.

In order to increase the security of medical data saved utilizing blockchain technology, a convolutional neural network (CNN) can be deployed. Data encryption, access management, and validation can be greatly aided by the CNN. An overview of the integration of a CNN model into a blockchain-based system for medical data protection is provided below:

Step 1: Data preprocessing and encryption

Preprocessing should be done on data before it is put on the blockchain to make sure it is in the right format. This could entail scaling, normalization, or noise reduction for medical photos.

Encrypt the information by using the CNN model. The CNN can create encrypted representations of the data instead of directly storing the actual data on the blockchain, rendering it unreadable by unauthorized users.

Step 2: Blockchain data storage

The blockchain should contain the encrypted data. There will be references to the encrypted data and associated access rights in the blockchain ledger.

The unchangeable record of transactions and data integrity provided by the blockchain make it tamper-resistant.

Step 3: Smart Contracts-Based Access Control

Use blockchain smart contracts to govern access control. These smart contracts can incorporate the CNN model to manage authentication. Authorized users could have to send data to CNN for decryption and validation against the smart contract's access criteria.

Step 4: Validation and Retrieval of Data

The smart contract can use the CNN model to retrieve data when an authorized user requests access to a specific set of medical records. Only if the user's request complies with the access permissions does CNN validate the user's request and grant access to the decrypted data.

Step 5: Audit and Monitoring

Keep an eye out for any unusual activity or attempts at unauthorized access on the blockchain network. Utilize blockchain's transparency and immutability to maintain an extensive audit record of all data-related transactions, including data access, sharing, and ownership changes.

Step 6: Strengthening Security

Put in place extra security measures to safeguard the CNN model, which is essential for data security. Assure that any vulnerability are patched and the CNN model is updated frequently.

Step 7: Regulation and Compliance

Ensure that all aspects of the system, such as the CNN model and blockchain, adhere to laws protecting patient data, such as HIPAA or GDPR.

Review and revise policies and procedures as needed to stay current with changing legal requirements.

6. IMPLEMENTATION PHASE

The framework for our proposed application, designed to enhance the security of medical data, consists of five main modules: Home, Register, Login, Hospital, and User. These modules collectively illustrate the functionality and performance of our application. Below, we provide a detailed explanation of each module and its role in ensuring the security of medical data.

1. Home Module:

The Home module serves as the entry point for users accessing our application. It prominently features the Login and Register options. The Login option allows both users and hospitals to access their respective accounts. The Home module sets the stage for a secure and user-friendly experience.

2. Register Module:

The Register module is a critical component for new patients or users who wish to use the application. It is mandatory for individuals who want to create an account. During registration, users provide their information and credentials, which will be securely stored and validated for future login.

3. Login Module:

The Login module is a common entry point for both individual users and hospitals. Users provide their credentials (username and password) to access their accounts. Hospitals log in with their valid credentials to manage patient data and monitor requests and updates.

4. Hospital Module:

The Hospital module is designed for healthcare institutions to securely manage patient data. Hospitals can log in using their credentials to access a dedicated dashboard. This dashboard allows hospitals to view the number of patients they are serving, track new patient requests, and monitor updates to patient information. The module ensures that hospital staff can efficiently manage patient data while maintaining data security and privacy.

5. User Module:

The User module is intended for individual patients and users. Patients who have registered can log in using their credentials to access their accounts. Once logged in, patients can securely interact with the application, update their medical information, and request services.

Data security is paramount, and patient information is protected using blockchain technology to prevent unauthorized access. In the past, patient data was often accessible to hospital staff without adequate security measures. However, in our proposed application, we prioritize data security by implementing blockchain technology. This ensures that sensitive medical information is not directly revealed, and access is tightly controlled. These modules collectively form the foundation of our application, providing a secure and efficient environment for storing and managing medical data while protecting patient privacy. The software requirement specification (SRS) outlines the framework and functionality of the upcoming product, ensuring that it meets the needs of users and healthcare institutions while maintaining data security.

7. EXPERIMETAL REPORTS

In this proposed application, we try to use Python Django as working platform and try to show the performance of our proposed application.

1) Home Page

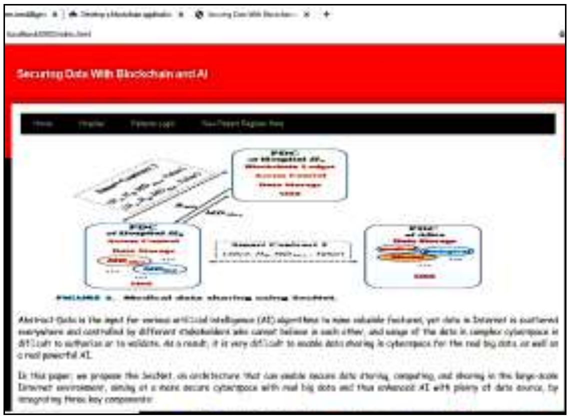
Securing Data With Blockchain and AI
Home
Hospital
Patients Login
New Patient Register Here

FIGURE 1. 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:

In the above web page we can clearly see the website contains three main modules such as : Hospital, Patients Login and New Patients Registration.

2) Hospital Login to Access Patients Data

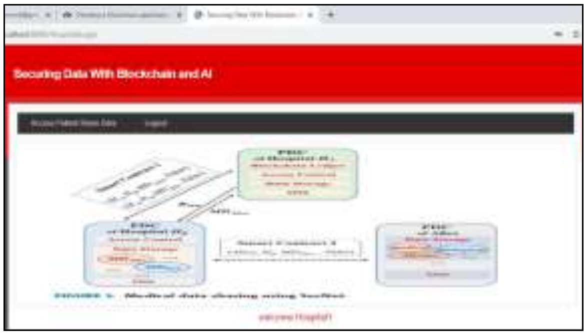
Securing Data With Blockchain and AI
Access Patient Share Data
Logout

FIGURE 1. Medical data sharing using SecNet.

welcome Hospital1

In the above web page we can clearly see the hospital login is successful by concern hospital authority and in existing days once the hosp admin enters into the account,he/she can access all the patients information which is available in their database.But now as we are applying AI with block chain the hospital staff cannot directly access the patients data.

3) Access only UnSecure Information

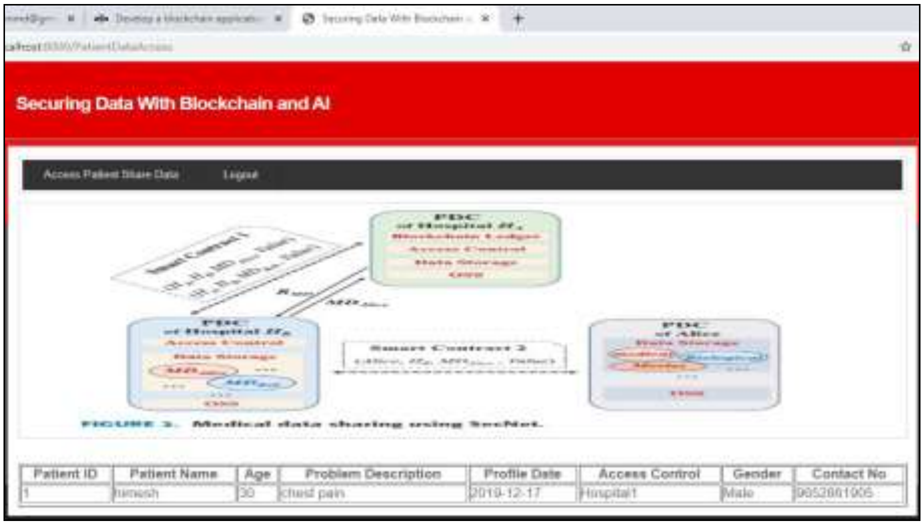

FIGURE 1. Medical data sharing using SecNet.

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No
1	himesh	30	chest pain	2019-12-17	Hospital1	Male	9052861905

In the above web page we can clearly see the hospital login is successful and after login they can only see useful information only from the hospital they can't able to see all the hidden information which is present in that patient record.

4) Patient can access his/her information with Block Chain Hash Code

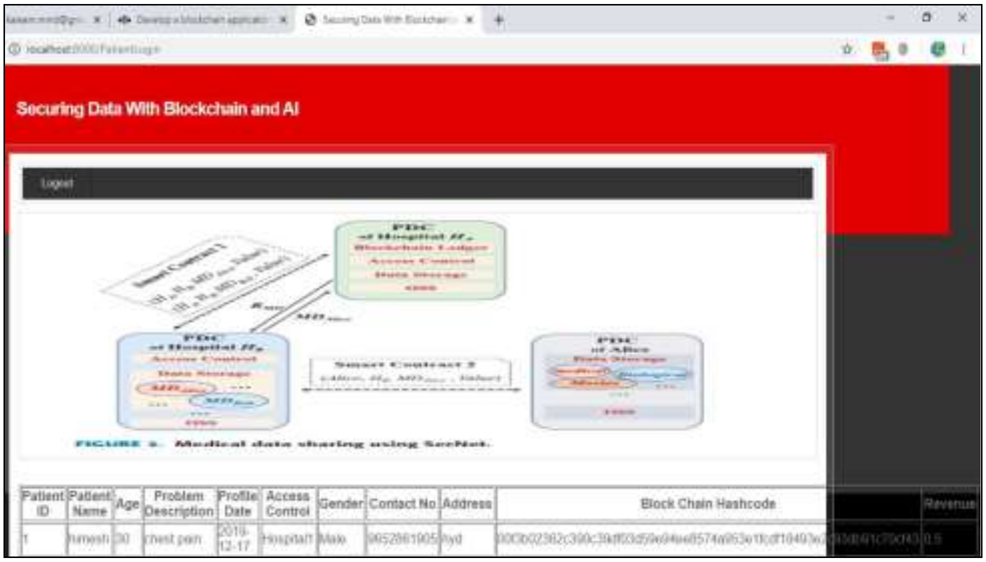

FIGURE 5. Medical data sharing using SecNet.

Patient ID	Patient Name	Age	Problem Description	Profile Date	Access Control	Gender	Contact No	Address	Block Chain Hashcode		Revenue
1	himesh	30	chest pain	2019-12-17	Hospital1	Male	9652861905	hyd	0003b02382c390c39df03d59a94ee8574a953e1fcdf16493e2	93d841c70d43	0.5

In the above web page we can clearly see the patient login is successful and after login he can see his personal information by entering the Block chain hash code which is present with him.

8. CONCLUSION

Using Block chain and AI to hit the tricky problem of data abusing for achieving trust in trustless environment we are using SecNet is the emerging model penetrating towards privacy preservation and security of data, sharing data of only required and hiding some data from disclosing to unauthorized users. SecNet works tremendously for guaranteeing ownership of data by using AI technology and Block chain technology and also getting good network security. It can be useful in medical systems as patients data is crucial. It can be also useful in financial data of customers. It is also resistive for DDOS attacks.

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. 112fi117, 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. 1656fi1665, 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. 1fi6.

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. 34fi42, 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. 44fi53, 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. 55fi61, 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. 21fi27, 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. 8fi14, 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. 14757fi14767, 2017.

11. D. E. O'Leary, ``Artificial intelligence and big data," IEEE Intell. Syst., vol. 28, no. 2, pp. 96fi99, Mar. 2013.

12. A. Halevy, P. Norvig, and F. Pereira, ``The unreasonable effectiveness of data," IEEE Intell. Syst., vol. 24, no. 2, pp. 8fi12, Mar. 2009.