REVIEW OF SECURING DATA USING BLOCKCHAIN

Dr DIVANU SAMEERA
Associate Professor,
BVRIT, Narsapur
sameera.d@bvrit.ac.in

G R SRINIVAS
Assistant Professor,
BVRIT, Narsapur
srinivas.g@bvrit.ac.in

G ANUHYA
BTech, Dept of IT
BVRIT, Narsapur
18211a1238@bvrit.ac.in

G SHIVANI
BTech ,Dept of IT
BVRIT,Narsapur
18211a1239@bvrit.ac.in

G NUTUHANA
BTech, Dept of IT
BVRIT, Narsapur
18211a1240@bvrit.ac.in

ABSTRACT

Data is an input of various artificial intelligence (AI) algorithms to get valuable features, but data on the Internet is scattered anywhere and managed by various stakeholders who are unbelievable, and complex It is difficult to use cyberspace data. As a result, it is very difficult to enable data exchange in the cyberspace, as well as true large data and true powerful AI. This article tells about SecNet architecture that enables , secure data storage, suggesting parts of the largest Internet environment for more secure cyberspaces with actual large data, and thus many data sources of AI and It can be improved by integrating three components one is Block chain-based data exchange with real estate maintenance guarantee that shares reliable data sharing in the largest environment to form substantial data. And another one is using AI Secure Computing Platform for producing smart safety rules than building a trusted cyber space. And also Trusted Value Exchange mechanisms provide a way to obtain economic rewards to promote data exchange to provide a way to promote data and services . In addition, we describe a typical deployment scenario of SECNET, as well as potential alternatives to analyse its effectiveness from network security and economic side.

1.INTRODUCTION

All data created must be stored in a location that cannot be modified or destroyed. Because these are valuable lessons learned from a person or a person's life or a group that can help the seed move forward. This has led people to collect and store a lot of data on different subjects, which has accelerated it.

The invention of a printing press that made it possible to acquire information in the form of a book that can be stored for a very long time. When the Internet was invented, another revolution in data storage, retrieval, and access took place. By then electronic storage had already been invented, but the Internet has emerged.

Another factor in this is that the Internet has enabled different computers and computing devices around the world to connect and share information. That is

Is designed to facilitate the exchange of information between researchers over long distances to avoid being physically present in the field to use resources. With the initial success, the Internet was opened to the public, and various services with the Internet as the backbone became popular. The Internet began to grow exponentially as more users and machines were connected each day. People are increasingly using the platform, which has increased the number of users who interact online. The internet grew up on social media and educational portals

The astronomical size and the data generated daily has grown to a tremendous size. With the increase in data and online users, an environment has been created to nourish people.

Learn and share valuable skills and information from around the world. The biggest drawback of having open access for everyone on the Internet is that some individuals also have it.

Malice that can ruin the experience of others solely for personal gain.

Many users on the Internet have valuable and sensitive data with personal data stored in the database .

Different organizations have internal data It is stored electronically in secret. This will result in an attacker could access this information .As a result, not only is it less secure, but it is also significantly less secure and loss to the organization. This is a problem as there is nothing Storage alternatives and convenience provided database. so, it is very important to provide ways to control access for the sensitive data only by trusted employees and other organization members can access data based on those hierarchies. This gives rise to the proposed blockchain paradigm. This technology was developed by a group of scientists in the late 1990s .Originally developed for use by digital notaries ideal for preventing document tampering. The paradigm is creation of the world's first cryptocurrency. Because it's strong due to its tamper-proof and decentralized nature cryptocurrency. Blockchain is one of the safest can provide very high security with the application since it is saved data, it can be used by one to protect your data and be efficient and effective access control mechanism for as well confidential data for your organization. Different reliable relationships between stakeholders of different data is a significant combination of Internet data exchange, and the data used for AI training or analysis is limited to the amount of amount and partial increase. Fortunately, the rise in Blockchain Technologies has an efficient and effective way to share trust data that can participate in a reliable environment. SECNET uses Kain Technologies of emerging blocks to prevent data abuse and enable

reliable data exchange in untrusted environments. For example, coordination can cooperate between different edge circulation paradigms to improve all system performance of the edge network [3]. Blockchain can enable reliable mechanisms is to be able to provide transparent and tampered -pull metadata infrastructure to significantly recode the data uses[6]. SecNet can apply advanced artificial intelligence technologies in the operation support system to adaptively identify the most suspicious data-related behaviours which are new too. swarm intelligence can be used in SecNet to further improve data security, by gathering various security knowledge from a large number of intelligent agents . throughout the CPS, using a trust exchange for incentive tokens [8].

2. RELATED WORK

Data safety is amongst key issues of any community architectures, and is the bottom for AI algorithms to enhance because of its requirement for large quantity of records from as a lot as feasible locations in Internet. Meanwhile, with a extra effective AI, records safety may be similarly covered at a better stage as an better AI can discern out superior and complex threats extra without difficulty than ordinary AI.

To better the safety of records in CPS, numbers of efforts are conducted. The work in [1] provides an structure named Amber to allow decoupling records from the internet packages, which offers manage cap potential to internet customers over their non-public records, in addition to presents a effective internet-huge question characteristic to look non-public records. To amplify the decoupling mechanism of records and packages from simplest internet offerings to all sorts of packages, the studies institution from the Media Lab in Massachusetts Institute of Technology designs the openPDS [5], performing as a secured digital area for customers to collect, shop and manipulate their records, isolating all sorts of packages.

Besides, the rising blockchain generation presents an green and impact manner to assure the safety of records in CPS, via way of means of supplying tamper-evidence and traceable recording capabilities in addition to incentive mechanisms. The authors in [2] increase the OriginChain machine to recognize the transparency and tamper-evidence capabilities of the metadata whilst the deliver chain line. OriginChain allows all associated events to acquire the equal relied on records and adapt to dynamic surroundings and regulations. The authors in [7] advise a blockchain-primarily based totally MeDShare machine to efficiently manipulate and shield scientific records, in addition to percentage scientific records amongst cloud repositories, with ensures on records provenance, auditing. The work in [6] overviews the historical past of blockchain and Intrusion Detection System (IDS) in details, and discusses the way to follow blockchain technology to IDS. Besides, the work in [4] designs a blockchain-primarily based totally incentive mechanism for crowdsensing packages, with privateness maintaining and records safety is ensured.

3.EXISTING SYSTEM

Now a days many networks or clouds will store user's data and they can sell that data to other organizations for their own benefits and user has no control on his data as that data is saved on third party servers.

Many users on the Internet have valuable and sensitive data with personal data stored in the database .

Different organizations have internal data It is stored electronically in secret. This will result in an attacker could access this information .As a result, not only is it less secure, but it is also significantly less secure and loss to the organization. This is a problem as there is nothing Storage alternatives and convenience provided database. so, it is very important to provide ways to control access for the sensitive data only by trusted employees and other organization members can access data based on those hierarchies. This gives rise to the proposed blockchain paradigm.

3.PROPOSED SYSTEM

This project introduces the SecNet architecture. This architecture can be used for a variety of purposes, including: B. Approve the storage of secure data, calculate raw data and share it with large internet domains. The main focus of real-world raw data is integrated with cyberspace and advanced artificial intelligence through three key components. Blockchain: Blockchain is a technology that guarantees ownership to join large domains that enable real data and contribute to the formation of true big data.

Every user data is stored in the form of blocks so it becomes difficult or impossible to change or hack or cheat the system. .

Proof of work algorithm used in mining process which will generate a hash value using SHA256 algorithm.

Here the hash function will convert the user data into hash value, using this hash value it is impossible to revert back to the user input data

in proof of work it will compute hash code using

This is a mechanism where we can purchase the services of Security, it encourages the sharing of data and it leads to the high performance of AI and also provides a economic rewards for successful service.

4.IMPLEMENTATION

project modules:

Our application includes the following modules

Patient Module

Hospital module

Patient module

1) Patient: After opening the application, the patient first creates a profile using everything

Illness information. Then the preferred hospital where he / she wants to subscribe to his / her data is selected. While creating the patient profile application itself, I created a blockchain object with all the permissions granted so that only those hospitals could access the patient data.

Patient Login Page: Patients can typically log in to the application with their profile ID and see the overall rewards earned by sharing data.

Hospital Module

2) Hospital Login Page: This application

used two hospitals, Hospital 1 and Hospital 2. At these hospitals, patients can share data with either or both hospitals. Each of the two hospitals can access patient data for common illnesses or disease names at any time by logging in to the

application and entering a search term. The AI ruleset takes the input for the disease string , performs a search operation on all patients, retrieves the corresponding patients, and has valid permissions for this hospital to access the data. I am. Determine if you are. Confirmation. If the hospital has permits, the application screen will display the patient record for that hospital. This is a code instance for creating a blockchain object in Patientd.

IMPLEMENTATION OF APPLICATION

Start creating the database with MYSQL by copying and pasting the content material from DB.txt to MYSQL. The configuration file has tradeport numbers from 3308 to 3306, and the views.py file has tradeport numbers for 3306.

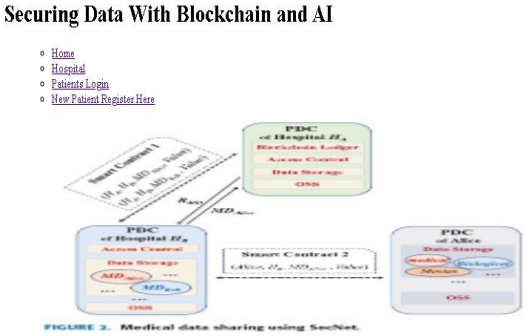

Figure 1.

After the above process, the application will open and you will see a link on the screen. Click this link and then click Register New Patient Here.

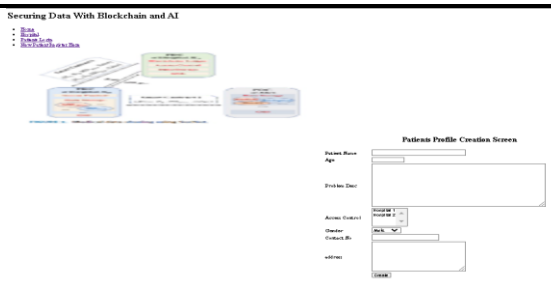

Figure 2.

The display screen allows you to select the hospital of your choice, including details of the affected patient`s illness. B. "Hospital 1". If the patient wants to select both hospitals, the patient can select two hospitals while holding down the "CTRL" key. When the entire process is complete, click the Create button to create the profile. You have now profiled the patient by providing the details with the patient ID as 1. Hospital 1 can then log in to the application to search for affected patients and obtain permission.

details for patients who agree only with Hospital 1

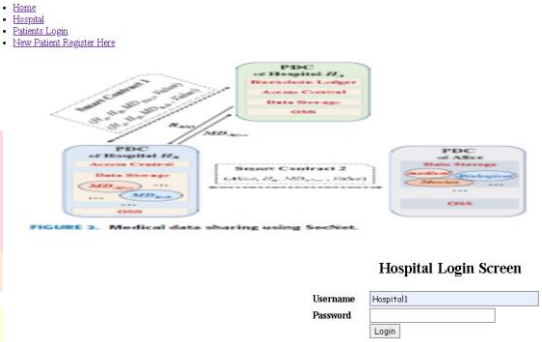

Figure 3.

Next, open the hospital login screen and log in with your username as "Hospital1" and your password as "Hospital1". To log in to Hospital2, use your username as "Hospital2" and your password as "Hospital2". After logging in, you will see another screen called "Welcome Hospital 1". Then click Access Patient Shared Data on the same screen to start searching for patient data.

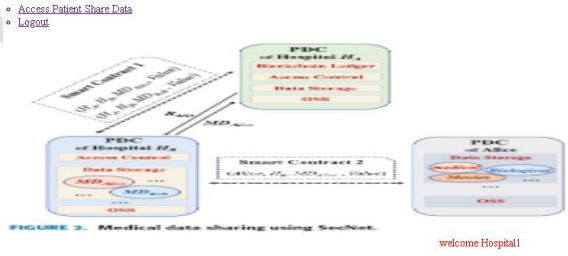

Figure 5.

Suppose Hospital 1 wants to find all patients with a illness named "fever" or "pain", enter them and click the "Credentials" button to move to another screen.

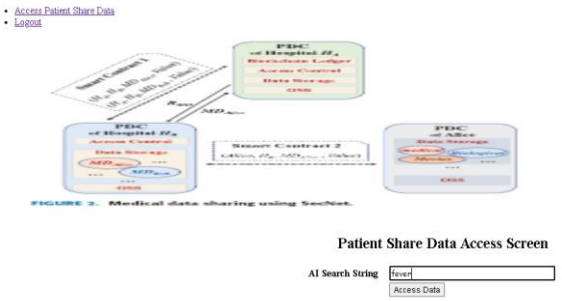

Figure 6.

Eventually, Hospital1 will get all patient details, but Hospital2 will not be able to view these details because Hospital2 does not have permission to access this data.

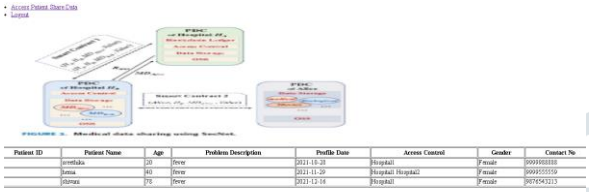

Figure 7.

To verify that Hospital2 is not authorized, first log out of Hospital1 and then log back in to Hospital2.

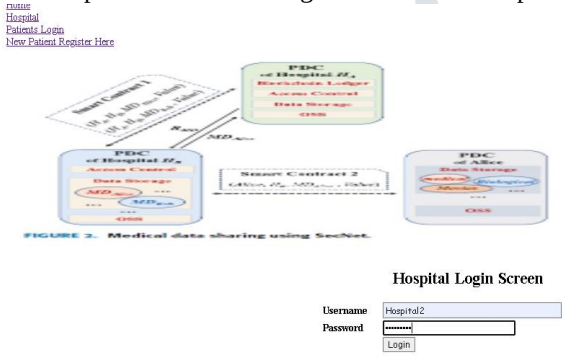

Figure 8.

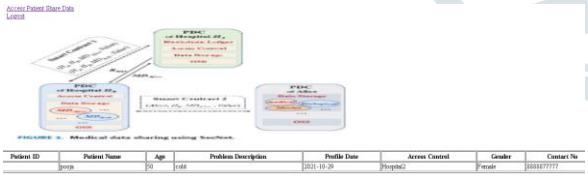

Figure 9.

In conclusion, blockchain is only available to users who have permission to access the data. Then enroll as a patient in the application.

First, enter your patient ID to log in as a patient and click Enter. All data related to the patient is then displayed on the screen with this hashcode generated by the blockchain, with a column called Premium Revenue showing points each time the patient completes the details shared with the desired hospital. I have.

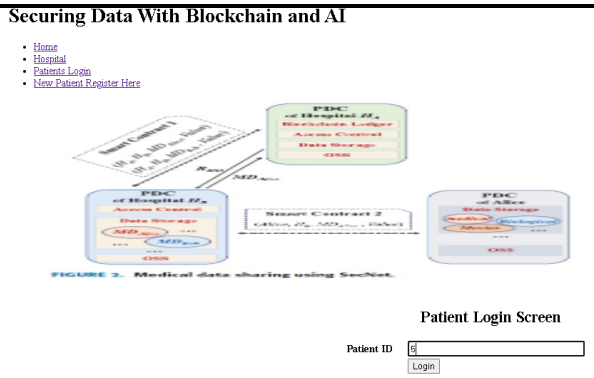

Figure 10.

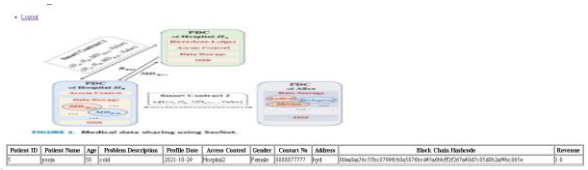

Figure 11.

In the Figure 11 above you can see all the details of the patient and the hash code generated by the blockchain. In the last column, the patient's premium income is 0.5, which is updated every time the hospital accesses it.

RESULT

Our application suggests that not all cyber information is publicly available. To solve the problem by making the data private only, we described a concept called a private data center (PDC). It uses blockchain and AI technology to provide security and trust to user information. In our project, patients can profile on the login page and select only the hospitals with which they want to share disease data. In this way, only hospitals that have permission to access patient data can access it.

CONCLUSION

A brand new network that uses AI and blockchain to tackle the problem of information misuse. The AI for reliable information control in unfamiliar environments. We recommend the SecNet paradigm. We specialize in storing, sharing, and processing information, not communications. SecNet uses blockchain technology and an AI-based, fully stable computing platform, as well as a complete blockchain-based stimulus mechanism that brings together information to provide a more effective AI paradigm and incentives. Ensuring ownership of information. It also describes the normal use of SecNet in a

hospital treatment system and provides options for using SecNet's garage features. Finally, we have developed an application that uses BlockChain-based data sharing with guaranteed ownership. This also enables reliable data exchange. AI runs the logic to see if the requesting user has permission to access the shared data.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] A. Halevy, P. Norvig, and F. Pereira, ‘‘The unreasonable effectiveness of data,’’ IEEE Intell. Syst., vol. 24, no. 2, pp. 8–12, Mar. 2009.

[8] 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.