ISSN: 2278-4632
Vol-12 Issue-01 No.01: 2022

SECURING DATA WITH AI&BLOCKCHAIN

Dr. Syed Sadat Ali Alias Abdul Gani M.tech, Ph.D

Professor, Dept. of CSE,Nimra College of Engineering & Technology, Vijayawada, AP

KAMALAPURAM SAIF ALI KHAN[1], JANDRAJUPALLI VIJAY KUMAR[2], ANNAM KARTHIK [3], SYED SAMEER [4]

[2,3,4,5]Student, Dept. of CSE,Nimra College of Engineering & Technology, Vijayawada, AP

ABSTRACT

Recent increases in security breaches and digital surveillance highlight the need for improved privacy and security, particularly over users' personal data. Advances in cybersecurity and new legislation promise to improve data protection.

Blockchain and distributed ledger technologies provide novel opportunities for protecting user data through decentralized identity and other privacy mechanisms. These systems can allow users greater sovereignty through tools that enable them to own and control their own data.

Artificial intelligence provides further possibilities for enhancing system and user security, enriching data sets, and supporting improved analytical models.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 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 orservice.

INTRODUCTION

The amount of personal data being collected is rapidly proliferating. Enterprises and governments use this data to profile individuals and to predict and control their attitudes and behavior. This can result in customized experiences, personalized services, and more efficient use of resources. It can also result in misinformation and exploitation by the entity that collected the data or by others that purchase or steal it.

In response to increases in cybercrime and growing consumer concern, legislation to protect personal data is being proposed and implemented. Organizations trading in personal data face increasing costs associated with managing and securing data.

They also face increasing risks that data will be misused or stolen, and that they will face legal or financial consequences, as well as damage to both their reputation and to relationships with customers and other stakeholders.

These systems can also reduce cybersecurity threats. privacy solutions by enabling users to better manage their data and by ensuring that data and models derived from the data are more accurate, fair, and reliable.

EXISTING SYSTEM

- In existing system data protection mechanisms such as encryption was failed in securing the data from the attacker.
- It does not verify whether the user was authorized or not.

PROPOSED SYSTEM

- The proposed system enables Private Data Centers (PDC) with the Blockchain and AI technique to provide security to user’s data.
- Blockchain-based data sharing with ownership guarantee, which enables trusted data sharing and generates hash code(unique).

IMPLEMENTATION (MODULES)

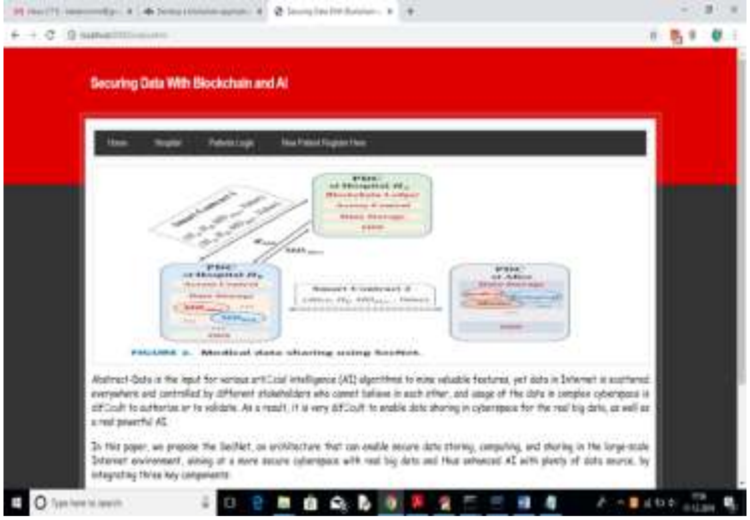
- **Patients:** Patients first create his profile with all disease details and then select desired hospital with whom he wishes to share/subscribe data. While creating profile application will create Blockchain object with allowable permission and it will allow only those hospitals to access data.

- **Patient Login:** Patient can login to application with his profile id and check total rewards he earned from sharing data.

- **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.

SAMPLE SCREENS



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

FIGURE 2. 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

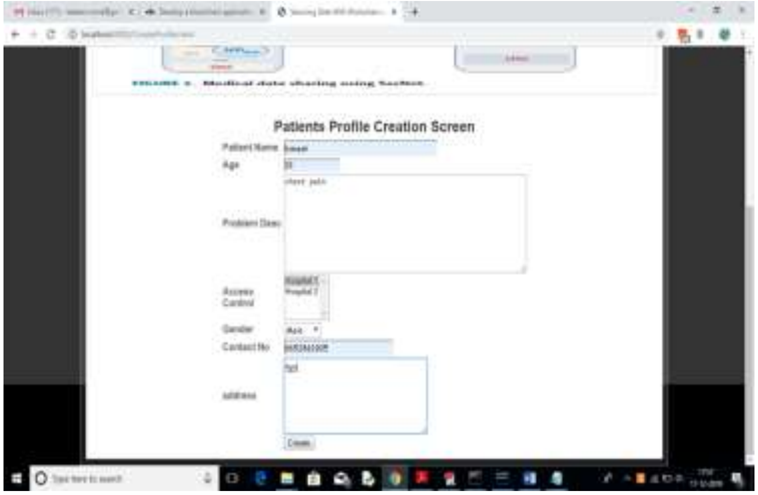
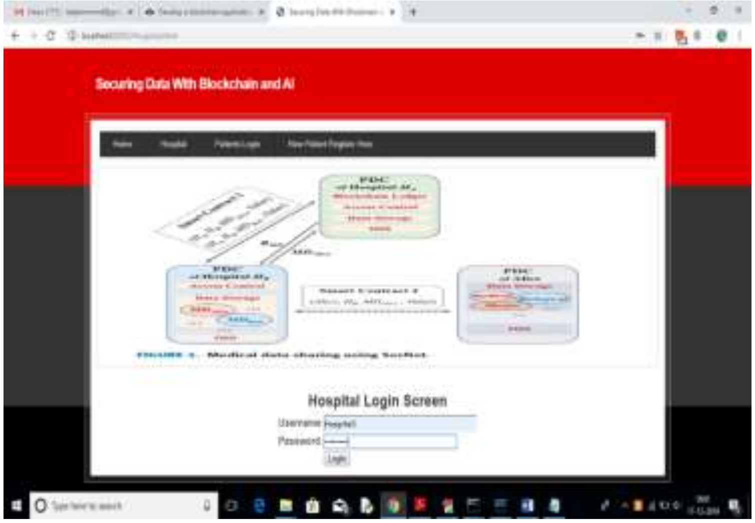


FIGURE 2. Medical data sharing using SecNet.

Patients Profile Creation Screen

Patient Name: kiran
Age: 35
Problem Desc: chest pain
Access Control: Hospital1, Hospital 2
Gender: Male
Contact No: 9652461008
address: hyd

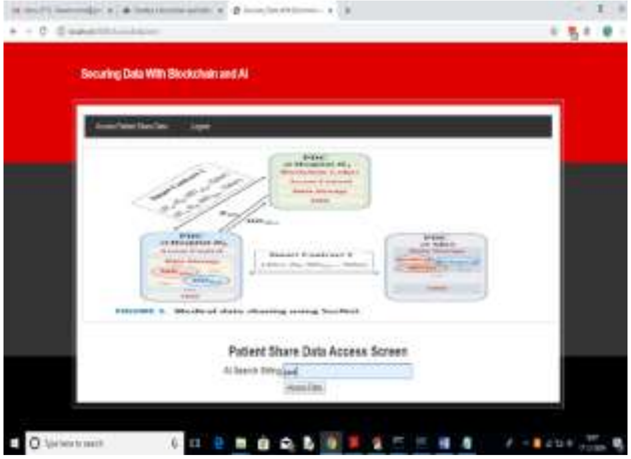


Securing Data With Blockchain and AI
Home
Hospital
Patients Login
New Patient Register Here

FIGURE 2. Medical data sharing using SecNet.

Hospital Login Screen

Username: hospital1
Password: ••••••••



Securing Data With Blockchain and AI

Patient Share Data Access Screen

CONCLUSION

Blockchain and AI technologies are improving at a rapid pace and enabling possibilities for sharing and combining data in ways not previously envisioned. Personal data, when shared, present a conundrum for firms and individuals, which can provide valuable benefits but can also create great risks and costs for both the individual and the organizations with which individual data are shared.

Blockchain provides new mechanisms, such as decentralized identities and zero-knowledge proofs, that enable data to be shared in ways that maintain the privacy of the individual and allow users to maintain control over their own data.

Blockchain participants can realize these outcomes through careful development of governance frameworks and mechanisms.

REFERENCES

- Risk Based Security. 2020 Year End Report: Data Breach Quick view. [Internet]. (2021). Link: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf

- Kellerman R. Five of the Biggest Data Breaches of the 21st Century. STAGE2DATA. [Internet] (2020) Link: https://www.stage2data.com/five-of-the-biggest-data-breaches-of-the-21st-century/

- Fruhlinger J. Equifax Data Breach FAQ: What Happened, who was Affected, what was the Impact? [Internet] (2020) Link: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

- Statista, Figure 1. Cybersecurity Breaches and Record Exposure [Internet] (2020) Link: https://www.statista.com/statistics/273550/databreachesrecorded/