Juni Khyat
(UGC Care Group I Listed Journal)
ISSN: 2278-4632
Vol-13, Issue-08, August 2023

PROTECTING DATA USING ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

[#1]GONE SATHISH KUMAR,

[#2] P.SATHISH, ***Assistant Professor,***

[#3]Dr.V.BAPUJI, ***Associate Professor& HOD,***

Department of Master of Computer Applications,

VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR,TELANGANA

Abstract: Data is the input for various artificial intelligence (AI) algorithms to mine important characteristics, however data on the Internet is distributed and controlled by various stakeholders who do not trust each other, and data usage in complicated cyberspace is difficult to allow or confirm. As a result, enabling data sharing for real vast data and genuine powerful AI in cyberspace is extremely difficult. In this paper, we describe SecNet, an architecture for secure data storage, computation, and sharing in a large-scale Internet environment. This architecture promises to deliver a more secure cyberspace with real big data and, as a result, improved AI with a large number of data sources. 1) Blockchain-based data sharing with ownership assurance, enabling trusted data interchange in large-scale situations to generate true big data. 2) A safe computing platform based on AI that develops more intelligent security rules to give a more reliable online environment. 3. trusted value - an exchange method for paying for security services that allows participants to get monetary compensation for sharing their data or services, hence boosting data sharing and increasing AI performance. In addition to presenting SecNet's common use cases and possibly further deployment options, we assess its success in terms of network security and financial gain.

***Keywords*:** SectNet, Blockchain, AI, Security

1. INTRODUCTION

The trend toward merging cyber, physical, and social (CPS) systems into a highly interconnected information society beyond just a digital Internet is becoming more apparent as information technologies develop. The owner of one's data in an information society should have complete say over any and all uses of that data. However, this is not always the case.

Data is undeniably the lifeblood of the information era, therefore it stands to reason that most major corporations would do well to collect as much data as they can in the near future. The built-in sensors in the devices of these huge firms are discreetly collecting more and more personal information, including location data, web surfing patterns, phone calls, and user preferences. This poses a severe risk to the confidentiality of the individuals whose data is being gathered. Furthermore, there is no reliable mechanism to monitor who is utilizing these data and for what purpose, and there are few options for punishing those who violate the regulations.

If data from the entire CPS can be quickly and reliably collected and combined, artificial intelligence (AI) will be able to outperform humans in more domains. This is the beginning of true big data. Because AI can process massive volumes of data and information simultaneously, this is the case. This offers many advantages (including improved data security) and allows AI to perform many tasks more efficiently than humans.

Data privacy is a major concern in SecNet

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

because users must make choices about where and how to store data in order to make use of particular services and applicationData protection innovation and application expansion are both significantly constrained by the current service techniques due to the inextricable nature of user data and applications. SecNet takes after HyperNet's Private Data Center (PDC) rather than openPDS's Personal Data Store (PDS). PDC's superiority in deployment and problem solving stems from its superior, more secure, and smarter data storage system, which is grounded in physical entities rather than software algorithms. Each PDC provides every SecNet user with a reliable repository for all of their data. With PDC on SecNet, users would know who is accessing their data, why, and how often. This would give them complete authority over all data operations and provide granular regulation of user access patterns. In fact, under some circumstances, SecNet can employ data-saving techniques other from PDC.

2. LITERATURE SURVEY

Lyu, Jiang, Jiang, Wang, Guo, Xing, & Yin, Rather than having all of your computers and networks in one central location, you can employ a hyper connected network. Patients' privacy was prioritized in the development of a lightweight RFID system for the IoT by W. Jiang, H. Li, Y. Yang, and K. Fan. For instance, Amber partitions user data from cloud services. Enhancing the ability to filter massive amounts of data.

Since AI algorithms require a large amount of data from numerous Internet sources, data security has emerged as a major obstacle for network designs to overcome. Data security is enhanced in a more substantial manner when a stronger AI is used since it can detect more complex threats in less time.

There are numerous different things the CPS does to ensure data safety. Amber is a framework developed to help individuals take charge of their personal data on the web by isolating it from their favorite online programs. This layout also features a powerful method of searching the web for specific user data. The Media Lab at MIT is responsible for developing the openPDS. By preventing any program from having direct access to the data, it provides users with a secure online space for doing so. The approach aims to make the system for decoupling data and programs universally applicable, not just to web services. OpenPDS incorporates SafeAnswer as well. SafeAnswer is a cutting-edge service architecture that instantly compresses sensitive information.

Additionally, the recently created blockchain technology provides an efficient and effective method of ensuring data security in CPS by enabling immutable, trackable records and incentive programs. The OriginChain strategy relies on the immutability and transparency of metadata to trace goods as they move along the supply chain. With OriginChain, everyone has access to the same high-quality information and can easily adapt to new requirements. Authors propose a blockchain-based MeDShare system for managing and securing medical records and for transferring medical data between cloud repositories with assurances of data provenance, auditability, and regulatory oversight.

The research takes a comprehensive look at both blockchain and IDS. Furthermore, it investigates the use of blockchain technology in tandem with IDS and draws sensible conclusions regarding the obvious risks associated with this area of study. The research also proposes an incentive system built on the blockchain that ensures the privacy and security of data in crowdsensing applications.

Because of its ability to sift through large amounts of data in search of hidden trends and then generate precise predictions, AI is also a useful tool for bolstering data security in CPS. The availability of large data and the advancement of computing power have made this a reality. The research delves deeply into the applications of both big data and AI, as well as future expansion opportunities like using AI to make data more safe.

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

This research demonstrates how AI performance can improve with access to more data for training purposes. More effort is required to create valuable datasets so that AI can better safeguard data. Also included in the article is a comprehensive analysis and evaluation of AI-based methods for cyber security. The project's ultimate goal is to launch a marketplace where users may buy and sell machine learning techniques in exchange for incentives. As a result, there will be more AI-based solutions for data protection, and the technology will be more accessible to a wider audience.

Everything discussed up to this point is geared toward keeping sensitive information safe. Making a blockchain tailored to the needs of certain applications, utilizing AI algorithms as an integral component of analyzing data security, and developing a new service paradigm that facilitates the separation of data and apps are all viable options. However, not a single one addresses data security from an architectural perspective. SecNet's goal is to improve the data security of all applications by integrating the benefits of AI and blockchain on a massive scale, and thus develop a universal networking design that can support the dynamic update of each of these functional components whenever it is necessary.

Existing System

The built-in sensors in the devices of these huge firms are discreetly collecting more and more personal information, including location data, web surfing patterns, phone calls, and user preferences. This poses a severe risk to the confidentiality of the individuals whose data is being gathered.

Furthermore, there is no reliable mechanism to monitor who is utilizing these data and for what purpose, and there are few options for punishing those who violate the regulations. To rephrase, it's difficult to handle the risks associated with the data you've obtained if you don't know how to manage it well.

Everything now in the digital era relies on data, and computers can only learn from information that has previously been gathered. Since the information is stored on servers that the users do not own, they have limited access to it. Some businesses, such as those that offer social media or cloud storage, may be able to store and resell users' personal information as technology improves.

Drawbacks:

1) Information provided by the user is not secure.
2) The individual is unable to access or modify his own data.

3. PROPOSED SYSTEM

To address this issue, we are implementing blockchain and AI in private data centers. There are three uses for it.

Blockchain:

The data users trade on the blockchain is completely secure. With this system, the user decides who may and cannot access his information. He may grant access to those who need it while denying it to anyone else. A user will be able to provide another user read-only access to data using blockchain objects.

ArtificialIntelligence:

Smarter security rules and a more reliable internet can be created with the help of AI-based systems for secure computing. Like a human brain, AI will employ logic to determine whether or not a user has access to shared data before granting access. If that's the case, AI will only admit the people you specifically authorize.

Rewards

Everyone who benefits from viewing info that has been shared will appreciate this method. It paves the way for information exchange with monetary compensation. This facilitates information sharing and enhances the performance of AI.

Advantages:

The user will have more say over his data, making it more secure and difficult to access for unauthorized parties.

4. IMPLEMENTATION

As a case study, we looked at the sharing of medical records**.**

The work on this project has been divided in half. Hospitals and patients the patient will provide a

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

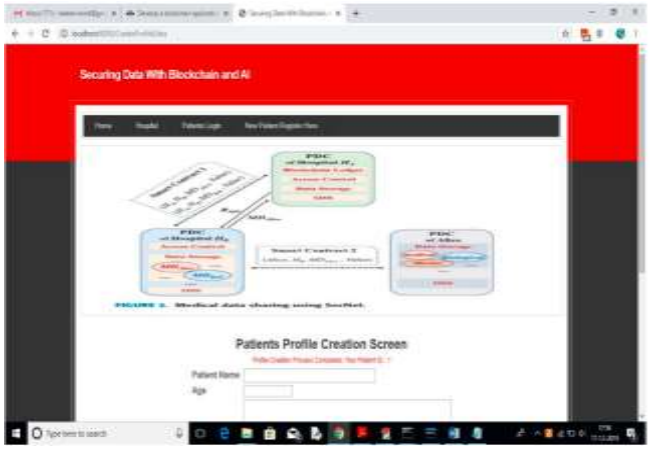
complete description of his illness and grant access to the desired organization. By creating a blockchain asset with the appropriate permissions, only the designated medical facilities will have access to the data. A patient's records may be shared throughout several institutions.

5. RESULTS

Ome Screen

To proceed to the next screen, select the "New Patient Register Here" button on the current page.

Patient enters his/her details



Patient Profile Creation Screen

Hospital Login Screen

Accessing Data from Patient

Patient Details

No patient data appeared on the final screen since Hospital2 did not have access to it. As a result, only authorized parties will be able to access data stored in a block chain. After that, use the patient ID to sign out and log back in as a patient.

ISSN: 2278-4632
Vol-13, Issue-08, August 2023

Patient Login Screen

PatientDetailsandhashcode

All of the patient's information, together with the hash code generated by the blockchain, is displayed on the screen above. The patient incentive income is now set to 0.5, as seen in the last column, but will fluctuate every time it is used by a hospital user.

6. CONCLUSION

We propose SecNet, a novel networking architecture that prioritizes the safekeeping, exchange, and processing of information over its transmission. This is done so that artificial intelligence (AI) and blockchain can be used to combat data exploitation and provide AI with the means to effectively handle data in untrusted settings. SecNet ensures data ownership by utilizing blockchain technologies. Long-term network security is enhanced by the inclusion of a blockchain-based incentive system, a paradigm and incentives for data merging, and more powerful AI. We also discuss the typical healthcare setting for SecNet and offer alternative storage recommendations. We also examine the novel concept of incentivizing users to help make a network safer by offering security guidelines, and we assess how well it makes networks less vulnerable to DDoS attacks.

FutureScope

Scientists will investigate the potential of blockchain technology for granting access to data in the near future. Create comprehensive and secure smart contracts for the computer services of SecNet that involve data exchange and artificial intelligence.

We will construct a prototype of SecNet and run extensive tests on state-of-the-art infrastructure to evaluate its viability.

References

[1] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu, and J. Xing,‘‘Hyperconnectednetwork:Adecentralizedtrustedcomputingandnetworking paradigm,’’ *IEEE Netw.*,vol.32, no.1,pp.112–117,Jan./Feb.2018.

[2] K. Fan, W. Jiang, H. Li, and Y. Yang, ‘‘LightweightRFID 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.VanDenHooff,M.F.Kaashoek,J.Mickens,R.Morris,andN.Zeldovich,‘‘Amber:DecouplinguserdatafromWebapplications, ’’ in *Proc.15th Workshop Hot Topics Oper.Syst.(HotOSXV)*,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, ’’ *IEEESecurityPrivacy*,vol.16,no.1,pp.3442,Jan./Feb.2018.

[5] Y. - A. de Montjoye, E. Shmueli, S. S. Wang, andS.Pentland,‘‘openPDS:Protectingtheprivacyofmetadatathrough SafeAnswers,’’*PLoSONE*,vol.9,no.7, 2014,Art.no.e98790.

[6] C. Perera, R. Ranjan, and L. Wang, ‘‘End - to endprivacyforopenbigdatamarkets,’’*IEEECloudComput.*, vol.2,no.4,pp.44–53,Apr.2015.

[7] X. Zheng, Z. Cai, and Y. Li, ‘‘Data linkage in smartInternetofThingssystems:Aconsiderationfromaprivacyperspective,’’*IEEECommun.Mag.*,vol.56,no.9, pp.55–61,Sep.2018