BioGecko Vol 12 Issue 03 2023

ISSN NO: 2230-5807

Data Privacy Using Blockchain and AI

Mrs. S. Mounasri[1], Dr. V. Anantha Krishna[2], Naruvadi Swetha[3], Byna Pravalika[4], Darnasi Saisindhu[5]

[1]Assistant Professor, Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India
[2]Professor, Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, India
[3,4,5]Computer Science and Engineering, Sridevi Women's Engineering College, B.Tech IV Year, Hyderabad, India

Abstract
Because of its distributed nature and varied stakeholders' lack of confidence in one another's stewardship, the complicated internet where it sits makes it impossible to authorise or validate its usage, despite the fact that it is the fuel that runs Artificial Intelligent algorithms. Therefore, it is difficult to promote data interchange in cyberspace for genuine big data and genuine strong AI. In this paper, we put forward the SecNet, an architecture that combines three key elements that allow safe storage, processing, and transmission in the large-scale Internet surroundings, with the ultimate goal of producing a safer online environment abundant in genuine big data, from which more robust machine learning could be derived. The first is the ability to share data securely in a large-scale setting with the assurance of ownership provided by blockchain technology, therefore generating authentic big data. 2) A secure computing platform powered by AI, with the potential to provide more nuanced security regulations and aid in the creation of a more secure virtual setting. Therefore, encouraging data to be shared and utilised a trusted benefit-exchange system for purchasing security services may lead to improved AI performance by giving participants the opportunity to receive monetary rewards for delivering their information or service. We also discuss the common methods of deploying SecNet and the many uses for it.

1. INTRODUCTION

More and more evidence suggests that the next step in the development of information technology will be the integration of computer network, palpably, and civilized technologies to create a extremely allied information band. In today's information age, a person's or company's data is a valuable asset that should be utilised only with their consent. Since information is the new currency, it seems to reason that large businesses would benefit from collecting as much information as possible. Inadvertently, the integrated sensors inmost the appliance from these major corporations are surreptitiously gathering an increasing amount of personally identifiable information, such location data, internet-searching action, customer calls, and user preferences. The absence of a reliable method for monitoring how and by whom the knowledge was used also leaves owners with little options in the case of abuse.

The ability to efficiently and reliably gather and combine the information dispersed throughout the entire CPS to structure real computer data is essential because AI is capable of handling massive amounts of information including massive information at the similar time, which has huge profits (such as accomplishing greater safety over info) as well as makes artificial intelligence (AI) acquiring the capacity to surpass mortal ability in increased areas.

2. RELATED WORK

"A Secure Computing and Communications Architecture for the Hyper connected Network"

The proliferation of IoT devices has led to the emergence of a highly developed CPS system that has the potential to become a robust data backbone. As a result of this loss of authority, it is very

challenging for CPS administrators to protect users' privacy, encourage new ideas, and guarantee data sovereignty. HyperNet is a game-changing decentralised trusted computing and networking technology designed to solve the issue of diminishing access to private data. An intelligent PDC, or digital duplicate, the decentralised reliable relationship connecting any company based on blockchain and programs stored on a blockchain, and the UDI podium, which allows for protected electronic object handling and an identifier-driven scatter appliance, all make up HyperNet. It has potential to usher in a data-driven future of computing because to its numerous advantages, including its ability to protect data sovereignty.

"Patient privacy in the World Wide Web of Things is protected using a low-power RFID protocol,"

Over the years, several cases have shown the fragility of the currently-used methods for protecting medical records from unauthorised access. Patients' privacy is jeopardised and medical advancement is stymied when sensitive information, such as patients' medical data, leaks to insurance companies. Parallel to the development of cloud-based computing and big data analytics tools, IoT innovation has accelerated. RFID is a key component of IoT infrastructure. Introduction of RFID technology into the healthcare sector may provide a practical solution to the trouble of medical confidentiality. The RFID tags in the technique may gather data using the reader, which can subsequently be sent to a back-end server for further processing. The whole process of exchanging data relies heavily on ciphertext. This research presents a straightforward method for shielding individuals' private data while using RFID tags inside the IoT infrastructure. The method ensures the confidentiality and safety of the collected information by using a robust authentication mechanism. Examining and analysing the procedure's security features has been found to effectively reduce the risk of confidential medical data falling into the wrong hands.

3. METHODOLOGY

Since protecting users' personal information is a high concern, we are using blockchain technology and artificial intelligence in isolated data centres to eliminate this risk. There are three functions it performs.

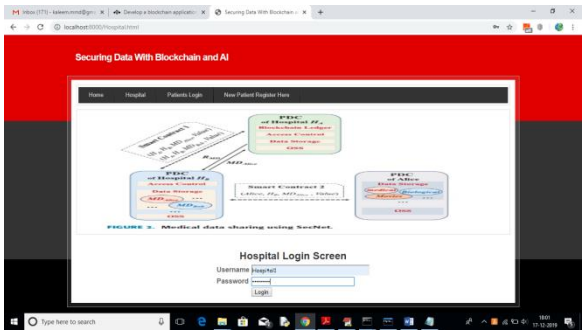
One: Blockchain, a distributed ledger that guarantees user privacy while exchanging data. As with any user permissions system, the data owner may choose who has access to his data and who does not using this way.

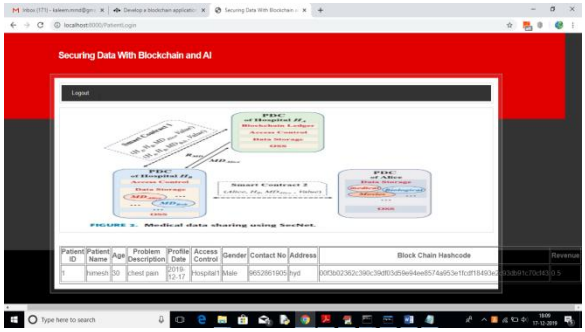
In a distributed ledger, only the user to whom access has been granted may see the data.

Second, AI-powered platforms for trustworthy computing provide more nuanced security regulations, and AI contributes to the development of a safer and more reliable virtual space. In the future, AI will do reasoning tasks like verifying a user's permission to access a shared database, much as the human brain does today.

4. RESULT AND DISCUSSION

I am now entering the patient's medical information and have chosen Hospital1 for submission; to submit both hospitals simultaneously, press and hold CTRL while choosing the second hospital. Create an account now by clicking the button below.





On the next page, you'll see the patient's full details as well as the hash code generated by the digital ledger, and the last column will show the patient's incentive earnings, which are going to be updated whenever a hospital user views the page.

4. CONCLUSION

To combat data abuse and provide artificial intelligence with the tools it needs to implement blockchain-based reliable information handling in a trust-less setting, we suggest an SecNet, a innovative networking architecture that prioritises secure information storage, communication, and aggregating over communication. SecNet is a decentralised network that leverages blockchain technology to ensure data ownership while also offering an AI-driven, blockchain-based safe computing platform with built-in incentives. The result is better network security since more data can be combined and more sophisticated AI can be created. We also go through a common use case for installing SecNet in the healthcare industry and provide a variety of different approaches to getting the most of SecNet's storage features. We also analyse its new strategy to encouraging users to exchange security rules for a better secured network, and we examine its efficacy in lowering network susceptibility to DDoS attacks. We want to look at the viability of utilising blockchain to approve data access requests and build protective agile contracts for information interchange and AI-based aggregating in Secure Networking in future studies. In inclusion, also model Secure Networking architecture & assess its usefulness by running expanded testing on cutting-edge systems (for instance, combining IPFS with Ethereum to create an architecture similar to SecNet).

5. 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. 112–117, 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. 1656–1665, 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. 1–6.

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. 34–42, 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. 44–53, Apr. 2015.
6. 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.