Volume: 10 Issue: VI Month of publication: June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44549

Blockchain and AI for Data Security in Distributed Systems

Ranjit Patnaik Sekharamantri[1], Krishna Narisetty[2]
[1, 2]Lovely Professional University

Abstract: Patients with hepatitis, influenza, cancer, and other deadly diseases are treated in hospitals in developing countries. In the event that a particular disease is encountered, staff can either refer the patient to an expert in that area or, in the absence of a diagnosis, may recommend the patient to the general physician. It is common for the general doctor to identify and eliminate an improbable disease by going through trial and error. A patient goes through this very painful ordeal as the doctors take one disease medication at a time to determine the cause of the symptoms. By using a Data Vendor, developed countries have largely addressed this problem. In this paper, we review all past work related to the provision of data security in networks, particularly those with data brokers. By introducing block chains and artificial intelligence, we can accomplish this best. An analysis of past data integrity methodologies in networks is presented in this article alongside an evaluation of a newer approach.

Keywords: Blockchain, Artificial Intelligence, Data Security, Cyber Security, Data Integrity.

I. INTRODUCTION

As soon as humans began to accumulate data, it became paramount that it was secure. A variety of sensory inputs received by different sensory organs have allowed humans to process information around them since the stone age era. The thirst for the unknown has led us to advance significantly in technology over the years, including paintings, music, textures, and many more. This thirst for the unknown has led us to expand into space and advance various arts such as paintings, music, textures, etc.

As these are valuable lessons learned throughout the lifetime of a species and that can be used to help the species advance, it is crucial that all of this data be stored somewhere that cannot be modified or destroyed. As a result, humans have collected and stored a huge amount of information over a broad range of topics and this has been accelerated by the invention of the printing press, which has enabled information to be preserved in books for a very long time.

As soon as the internet was invented, another revolution occurred in how data would be stored, retrieved, and accessed. By then, electronic storage had already been invented, but the internet had added another element to this, allowing computer and computing devices across the globe to communicate and share information with each other. In order to eliminate the need for researchers to be physically present at the location to utilize the resources, this program facilitates information exchange over a long distance between researchers. After the internet became a success, many services that depended on it as a backbone flourished as a result of its initial success. Every day, more and more people and machines are connecting to the internet, resulting in exponential growth. Users began interacting online more frequently as the platform was used more and more. As social media and educational portals increased in size, the internet became massive, and the amount of data created every day increased to an astronomical level. As the amount of data and the number of users online grew, it created a world-wide nourishing environment that allowed people to acquire valuable skills and share information.

People who have malicious intent can ruin other people's experiences for personal gain, as well as those who have open internet access. Many organizations also store their internal data electronically, which is confidential, in databases. As a result, there are many users on the internet who have personal and valuable information stored in databases. There is no alternative for storing and using the information, so there is an increased risk of an attacker gaining access to this information in a way that would compromise security and pose a huge threat to the organization. In order to ensure that only trusted employees and other members of the organization can gain access to sensitive data, based on their hierarchy, it is imperative to provide a mechanism for controlling access to sensitive data. In the late 1990s, a group of scientists proposed the blockchain paradigm, which was primarily designed for digital notaries as it is an excellent tool for tamper-proofing documents. The technique was originally developed as a method of creating digital notaries. Since it is tamper-proof and distributed, it is an ideal choice for a cryptocurrency since it was largely unused until it was applied to the creation of the world's first cryptocurrency. With its high degree of security, blockchains can be utilized to safeguard data and provide a very effective access control mechanism for sensitive information that is important to an organization. As one of the most secure applications, blockchains can provide a very high level of security for the data they store.

II. LITERATURE SURVEY

Based on a thoughtful evaluation of many authors' works, this section of the literature review finds the following facts.

As a result of the rapid pace of technological advances and the advent of the Internet of Things, S. Yu states that the number of smart devices connecting to the internet has increased rapidly. As a result of being connected and interacting with the internet, these devices generate a lot of data that cannot be processed efficiently. They generate a large amount of data that cannot be processed efficiently. This study proposes a low-cost alternative for creating economic value from the IoT data generated using an effective technique based on blockchain. Among the major disadvantages of this methodology is that large amounts of malicious data can be uploaded, resulting in its misuse.

Researchers also praised the robust security provided by the blockchain platform, pointing out that it is the foundation of network security construction. R. Wang elaborates on the PKI. To strengthen the Public Key Infrastructure, the authors have combined both methodologies by creating a permissioned blockchain that transforms it into a privacy-aware one. The key benefit of permissioned blockchains is improving the efficiency of certificate and configuration applications. However, the major disadvantage is that this has been a very specialized approach to the blockchain paradigm.

According to C. Ehmke, the blockchain paradigm has gained enormous popularity and limelight in recent years because of its use in financial applications. It has been widely adopted by researchers and implemented in a wide range of different fields, which has greatly improved the security of many applications by implementing the blockchain. To mitigate this effect, the authors have implemented a scalable and lightweight blockchain protocol that reduces the need for the user to download the entire chain.

In his book, R. Wang describes a video surveillance system as an indispensable tool for managing and surveying large cities. An environment information transmission system can be installed in the event that a video surveillance system is installed, so the individual does not have to travel long distances or be physically present. The IoT and Realtime monitoring have increased the monitoring standards, so they are susceptible to attacks. In order to ensure a seamless and secure video surveillance system, the authors developed a permissioned blockchain and Convolutional Neural Networks system. There has been no large-scale testing of the system and it will be in the future research to be performed.

Named Data Networking has been lacking a key management feature that is used by the producer to name every object and to digitally sign them, according to J. Lou. Conventional approaches have a number of disadvantages, including a lack of trust between the sites and the high likelihood that if the primary node fails, there will be failure. A key management scheme based on blockchain for Named Data Networking is therefore proposed in this paper by the authors. It is also important to note that the decentralized architecture can be very helpful in overcoming failures, as the blockchain increases the trust between sites. Despite being proposed, the proposed scheme hasn't been extensively evaluated for its ability to reduce NDN cache pollution.

In recent years, cryptocurrency has developed at an extremely fast pace, leading to a thorough examination of the paradigm, according to S. Wang. Using this method, a lot of irregularities were uncovered in the paradigm, such as Smart Contracts, which have caused the "DOA Attack" and resulted in a massive loss. The authors have thus provided a comprehensive and systematic analysis of smart contracts based on the blockchain paradigm. Authors provide a six-layer architecture for smart contracts but do not verify the security of the system. The authors provide a security-enhancing six-layer architecture.

A decentralized storage system based on blockchain technology is introduced by Y. Xu. Blockchain is a powerful idea for designing a highly secure decentralized storage system. Several blockchain protocols have been proposed by the authors to eliminate the storage problem that certain devices encounter. Because of its decentralized architecture and implementation of the Blockchain paradigm, the proposed methodology is highly resilient to failures and able to sustain heavy loads and optimizations gracefully.

In his keynote speech, M. Marchesi discusses how blockchain is developing rapidly and how ongoing research is occurring due to the growing interest in this paradigm and increasing demand. According to the author, this increased pressure has resulted in an increase in security lapses on the Ethereum platform as well as the cryptocurrency exchanges as evidenced by a number of incidents. As a result, the speaker also highlighted some of the numerous opportunities that can be achieved by the blockchain paradigm, including a reward and penalty scheme for developers that can be implemented with Blockchain tokens.

It is an innovative concept that has been proposed for the detection and identification of various money laundering schemes utilizing the blockchain framework. A. Maksutov elaborates on the Blockchain paradigm and its uses. In order to evaluate user participation, the authors used the proposed methodology for deanonymizing transactions and tracking coin join transactions. This information is used for determining whether the transactions are fraudulent or money-laundering operations.

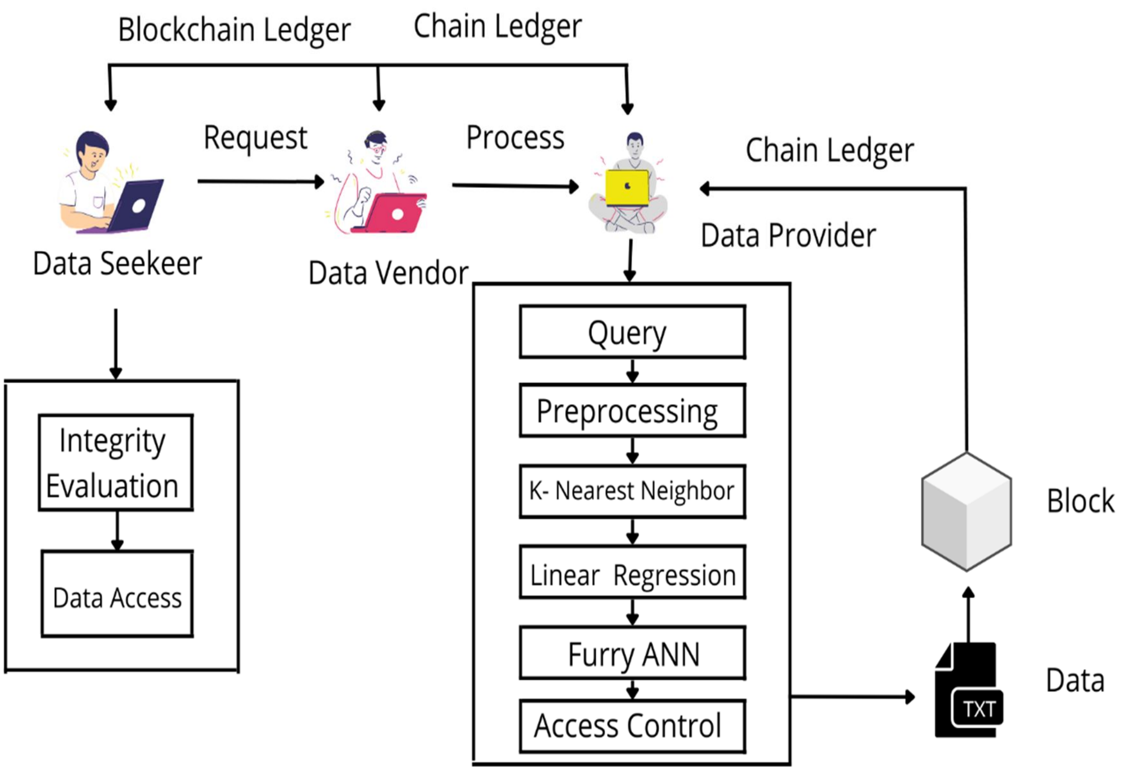
A problem with adding blockchain to existing platforms, according to F. Wessling, is that adding it is not the same as building applications from scratch by incorporating the blockchain into them.

By analyzing the attributes of blockchain, such as anonymity, trustlessness and immutability, the authors determine the amount of blockchain that will be required for various implementations. Based on the specific application and use case of the application, the authors have outlined various different processes utilizing various different elements of the blockchain technology.

In his explanation, J. Wang explains that most crowd sensing applications collect a large amount of data by using smartphones as a source of data. However, most of the time, users are under compensated for their contributions. In order to promote privacy and security, the authors developed an innovative reward and punishment scheme using trustless and secure blockchains that rewards users for contributing to the large data sensing paradigm. In this paper, there were no solutions discussed for possible collusion attacks, which is a serious concern.

A decentralized and secure Blockchain architecture has many advantages, according to S. Pandey. According to the author, there has been an increase in research being conducted in this field, and an increased interest has been seen in implementing blockchain technology to strengthen and secure existing systems. Consequently, the authors have developed an innovative and practical simulation tool for planning, stabilizing, and designing blockchain systems, applications, and networks. There are several drawbacks to BlockSIM, including the fact that it is an opensource, comprehensive, and accurate solution for blockchain simulations. A major drawback is that the authors did not model internet latency, which impacts the simulation's accuracy.

III. SYSTEM OVERVIEW DIAGRAM



IV. CONCLUSION

The public health record database and techniques have been used in this paper in several related works to achieve various different approaches and identify their shortcomings and flaws. An array of methods for managing Public Health Records have been proposed by a multitude of authors each offering their own unique approach. We have been able to use this insight to formulate a secure and efficient Public Health Record management system that uses Blockchain Principles. As a result of its inherent resilience to tampering and changes, Blockchains are used in the Public Health Record System to provide an effective Access control mechanism that helps to prevent the leakage of valuable sensitive patient data. In the upcoming studies, the discussed methodology will be used

REFERENCES

[1] S. Wang L. Ouyang et al, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019.

[2] M. Marchesi, "Why Blockchain Is Important for Software Developers, and Why Software Engineering Is Important for Blockchain Software", International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 2018.

[3] S. Pandey et al, "BlockSIM: A practical simulation tool for optimal network design, stability, and planning",. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019.

[4] R. Wang et al, "A Privacy-Aware PKI System Based on Permissioned Blockchains", IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), 2018.

[5] C. Ehmke, F. Wessling and C. Friedrich, "Proof-of Property - A Lightweight and Scalable Blockchain Protocol", ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, 2018.

[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. [8] Q. Lu and X. Xu, "Adaptable blockchain-based systems. A case study for product traceability," IEEE Softw., vol. 34, no. 6, pp. 21-27, Nov./Dec. 2017

[7] 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. 8-14, Jul./Aug. 2018.

[8] 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.

[9] Y. Xu, "Section-Blockchain: A Storage Reduced Blockchain Protocol, the Foundation of an Autotrophic Decentralized Storage Architecture", 23rd International Conference on Engineering of Complex Computer Systems (ICECCS), 2018.

[10] 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.