International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Maintaining Privacy in Block chain-Based Data Sharing

[1]Lavanya Mathiyalagi A,[2]Dr.R.Ravi, [3]Sarika K

[1]Assistant Professor, Computer Science and Engineering, Einstein College of Engineering, Tirunelveli.
[2]Professor/Dept. of CSE, Francis Xavier Engineering College, Tirunelveli.
[3]Assistant Professor, Computer Science and Engineering, Einstein College of Engineering, Tirunelveli.

ABSTRACT:

IoT systems that gather and process data are susceptible to risks to availability, integrity, and privacy, particularly those with centralised control. As a result, we offer a novel framework for safe IoT data sharing and privacy preservation in smart city settings, based on blockchain technology. Data from multiple sources is crucial to the development of media convergence. Its fusion processing opens up new avenues for the exchange and distribution of media data and permits additional data mining and value utilisation. On the other hand, it also has significant issues with maintaining user and data privacy. In this, we provide a multi-source data privacy protection approach based on block chain technology and homomorphic encryption, which addresses the issue of multi-source heterogeneous data privacy protection in media distribution and shortens the time required to process cypher text. Block chain stores data in sequentially connected blocks that are cryptographically linked to guarantee immutability.Every block is resistant against tampering since it includes a hash of the one before it. This feature guards against unwanted changes and guarantees the integrity of IoT data. Large-scale IoT data may be analysed by AI-powered algorithms to find trends, spot abnormalities, and anticipate any security risks. Through the ability to learn from data patterns, machine learning models can identify anomalous behavior in Internet of Things (IoT) devices, which may indicate a security compromise. Provably safe software is what is suggested. Its efficiency and practicality are demonstrated by performance analysis and experimental findings.

Index terms: Machine learning, IoT, Block Chain, encryption, decryption

INTRODUCTION

The safeguarding of privacy is significantly affected by the combination of block chain technology and artificial intelligence (AI). Furthermore, maintaining these solutions' privacy offers dependability and data security. The article provides an overview of AI and block chain, as well as the resulting privacy protection methods. It discusses k-anonymity techniques, multi-tier distributed ledgers, data encryption, and de-identification. It also evaluates the following five crucial areas of privacy protection systems for AI-block chain integration: scalability, permission management, data protection, network security, and access control. Additionally, it identifies deficiencies and recommends solutions to address them. This paper categorizes and describes privacy protection solutions using AI-block chain application scenarios and technical systems. Finally, upcoming privacy protection technologies from AI and block chain integration aim to improve efficiency and security, leading to more comprehensive privacy protection.

The pace of technological advancement is accelerating, surpassing even the predictions made some decades ago. To develop and deploy smart city prototypes—which include smart industries, houses, automobiles, transit, and other smart human devices—a great deal of scholarly research and industry adoption has been done. Many key technologies have contributed to this futuristic human civilization's development.

These technologies include cloud, fog, and edge computing, artificial intelligence (AI), Internet of Things (IoT), and software-defined networking (SDN). Furthermore, Block chain technology was able to add capabilities to those technologies that are necessary for the complete automation required in smart environments.

OBJECTIVES

- To guarantee the integrity and dependability of IoT data transferred on the block chain by keeping it unchangeable and impenetrable.
- To use cryptographic methods to safeguard sensitive data privacy, such as encryption and homomorphic encryption. This maintains secrecy and stops unwanted access.
- To lower the risk of privacy breaches by using decentralised identity management solutions to guarantee that the identities of users, IoT devices, and other entities stay anonymous.

Problem Overview

The platform strives to safeguard the identities of the Sender (S) and Recipient (R) in every transaction. Notice that by letting S use an ephemeral key to sign the transaction, you can easily safeguard its identity. But maintaining R's identity is a difficult task. It makes sense to send the transaction to a random address so that only R will be able to deduce that it is meant for them. To make matters more difficult, in our scenario, R additionally has to know who sent the message. For example, upon receiving data sharing, a data consumer must precisely identify the data owner in order to ascertain the PRE private key that corresponds to the data for decryption. In order to successfully solve the issue, we employ hidden keys and concealed transactions. It is assumed that a Sender (S) and a Receiver (R) wish to engage in a covert transaction.

Many data sharing systems use Ciphertext-Policy Attribute Based Encryption (CP-ABE), a sophisticated cryptographic primitive. CP-ABE incurs privacy concern despite its inherent appropriateness for data sharing systems. In particular, in CP-ABE, the data is encrypted using an access policy (P) made up of attributes and logical operators, and the user's private key is linked to its attributes set (S), which includes things like age and name. Any user can decrypt the encrypted text if their attribute set matches Pisable's. Thus, fine-grained access control over encrypted data is made possible by this approach. However, in order to aid the user in successfully decrypting the content, such an encryption scheme needs to be stored alongside it. Nonetheless, it is clear that data stakeholders' privacy is violated when P—which contains user attributes—is kept on a dishonest storage node. In order to use the benefits of CP-ABE without compromising privacy, we construct a CP-ABE system that supports hidden access policies derived from a revocable predicate encryption.

Block chain

Block chain is a safe, decentralized way to transfer data. With block chain technology, a particular group of parties can share data. It is able to gather and exchange transactional data from intricate sources. Information can be divided into blocks to enjoy together, linking by distinct identifiers in a single information source can guarantee data integrity, the encrypted hash mechanism, data security, and the elimination of data replication. A block chain is dependent on the distribution system, much like a transferred disk, and does not require a trustee or an outside party. The framework includes certain information that has been duplicated and registered in the registry, preventing information from being misplaced when there is just one intended point of irritation.

Proof of Work (PoW) is one of the continuous rules used by block chain to regulate options and produce new squares. Thus, from a computational standpoint, the information control is typically conflicting. Thus, the data entered into the squares doesn't change. In the block chain system, the exchange between two meetings can be efficiently controlled by different members. The owner of the information can monitor every interaction and utilize it indefinitely. As an illustration by agreeing to the fees for every piece of data that a stranger uses.

Data encryption:

Before being sent across a network or kept on a block chain, Internet of Things data is encrypted. This stops uninvited parties. From gaining access to the unprocessed data.

End-to-End Encryption:

Encrypt data from the point of generation by Internet of Things devices to the point of destination, guaranteeing its confidentiality. This stops data interception and eavesdropping during transmission.

Homomorphic Encryption:

In certain circumstances, computations on encrypted data may be done using homomorphic encryption without breaking the code. This preserves anonymity while enabling data analysis that respects privacy.

Public Key Infrastructure (PKI):

Utilize PKI to oversee encryption keys safely. Public-private key pairs can be used by IoT users and devices to facilitate safe data sharing and communication.

Decryption:

Authorized Access: The decryption keys are only accessible to those who have been given authorization. This guarantees that only those who are meant to receive can decode and get to the information. One way to grant access to particular parts of encrypted data is through the use of selective decryption methods, which can be implemented in accordance with access control policies or user permissions. This keeps private data from being unnecessarily exposed.

Identity-Based Encryption (IBE):

This method does not require explicit key exchange; instead, it decrypts data based on the recipient's identity.
This keeps security intact while streamlining key management.

SYSTEM STUDY

EXISTING SYSTEM

These are the actual hardware items in the Internet of Things ecosystem that gather data from diverse sources. Sensors, smart gadgets, and networked machinery are a few examples. These devices collect data, which they then securely transfer to the system for additional processing. They guarantee the data's validity and integrity. In order to protect privacy and security, the system securely transmits the data that is gathered from IoT devices. Homomorphic encryption algorithms are used to encrypt IoT data. Without having to first decode the data, computations can be done on it thanks to the encryption technique. A block chain, which offers immutability, transparency, and decentralization, is used to store the encrypted Internet of Things data. Data security and integrity are guaranteed by the block chain, making it impenetrable to manipulation. The AI module does a number of activities, including predictive modeling, anomaly detection, and data analysis. Without sacrificing privacy, it makes use of machine learning and other AI methods to extract insights from the encrypted data. the encrypted and processed data, guaranteeing data security and privacy.

Encryption keys and access control procedures make sure that only those you can trust can access your data. Because of the auditability and transparency offered by the block chain, stakeholders to monitor data access, changes, and provenance. This improves the system's accountability and sense of confidence. The encrypted data analysis is utilized to provide insights and make well-informed decisions using the processed data. The ensures the security of the sensitive data. Data security and privacy are ensured by limiting access to processed and encrypted data to authorized people or entities. Users or authorized entities can view the insights utilize the processed data, or carry out particular actions in accordance with their authorization.

Disadvantages of Existing System

- Data Tampering
- Loss of data.
- An attacker reading data without altering it.
- Data access by malicious cloud users (unauthorized individuals)

PROPOSED SYSTEM

The system proposes the actual physical objects in the Internet of Things ecosystem that gather data from different sources. Sensors, smart devices, and networked equipment are a few examples. The Internet of Things devices gather information and use homomorphic encryption methods to encrypt it. Computations on the encrypted data are possible thanks to the encryption technique, which keeps its contents hidden. The centralized system or a dispersed network of nodes receives the encrypted Internet of Things data safely.

On a block chain network, the encrypted Internet of Things data is kept. Data integrity and immutability are guaranteed by the decentralized, tamper-proof storage system offered by the block chain. On the block chain, smart contracts are used to specify the guidelines and requirements for accessing and exchanging IoT data. These contracts make sure that only authorized parties can access and use the data by enforcing data privacy and security regulations.

The AI module uses methods like fully homomorphic encryption (FHE) and secures multiparty computing (MPC) to process encrypted data without having to first decrypt it. It guarantees that the delicate Information is still kept private. Without disclosing the sensitive information behind the encrypted data, the AI module extracts insightful and useful information. Decisions can be made using these insights, or they can be disclosed to authorize parties. The decrypted insights and certain operations on the data can only be accessed by authorized entities or people who possess the required authorizations. Through openness and auditability offered by the block chain, parties may monitor data access, alterations, and provenance. It improves the system's capacity for accountability and confidence.

Algorithm used:

Ring Signature Algorithm:

Any member of a group of users who have keys can execute a ring signature, a sort of digital signature. A message bearing a ring signature, therefore, is approved by a member of a certain group of people. One of a ring signature's security features is that figuring out which member of the set's key was used to create the signature should be computationally impossible. Ring signatures are comparable to group signatures, but they are not the same in two important aspects: first, an individual's anonymity cannot be taken back, and second, any group of users can be used as a signing set without further configuration.

Homomorphic encryption algorithm:

A cryptographic technique called homomorphic encryption makes it possible to do calculations on encrypted data without the need for decryption. This means that when raw data is being processed, modified, and subjected to different algorithms and analysis, it can be completely encrypted. This lets you share data with third parties for processing without compromising its privacy. Homomorphic encryption is poised to open up a plethora of intriguing use cases, as existing encryption techniques are unable to perform calculations on encrypted data.

Advantages of Proposed System

The system is integrated with an AI module that can handle a number of functions, including predictive modeling, anomaly detection, and data analysis. The encrypted data is directly processed by the AI algorithms, protecting privacy and yielding insightful result.

- Data integrity and privacy threats
- Data Monetization and Ownership
- Reduced Costs and Improved Efficiency

SYSTEM IMPLEMENTATION

System Modules:

1.Signup
2.Login
3. Unique User ID (UUID) verification module
4.Transaction Module
5.Malicious Cloud User identification
6.Verification and Rewarding

Modules Description

1. **Signup:**
   - Any new user must first register their details to obtain their unique user id (UUID)
   - Registration or signup process is done using their e-mail and Password
   - On successful registration process, the system assigns a unique ID to the user
2. **Signin Module:**
   - To obtain their identity information, such as their UUID and tokens, any registered user who wants to conduct a transaction on the block chain network must log in each time.
   - For increased security, two factor authentications might be employed.
   - An OAuth2.0 token is used to securely process login verification.
   - Every time a user logs in, all information is recorded, including the date, time, and IP address.
3. **UUID Verification:**
   - UUID, which stands for Unique User Id, is assigned to every user and is completely unique. For increased security, this UUID varies over time.
   - The UUID is continually checked to ensure that every request is legitimate.
   - The transaction request would be promptly cancelled if the UUID didn't match.
   - The UUID is regenerated and the verification procedure is repeated if the algorithm detects anything questionable.
4. **Transaction Module:**
   - The file uploading procedure is started and completed following the UUID and OAuth2 verification.
   - Before completing the transaction, the file undergoes checksum verification.
   - A token id is returned following a successful file upload to the server, and it will be cross-checked with the awarding system.
5. **Malicious Cloud User identification:**
   - This module constantly interprets the client or End User request with the UUID
   - This module classifies the requests either a valid or invalid request
   - The Malicious Cloud User is identified using Homomorphic algorithm
   - If the request is found to be from the MCU, the system would abort the transaction request to the server.
6. **Verification and Rewarding:**
   - This module waits for a successful transaction initiation.
   - Once the request was successful, the system verifies the token which was returned during the upload process
   - Furthermore, we use RING signature to ensure the verification.
   - If everything is fine, the Cloud User is rewarded for their token

RESULTS AND DISCUSSION

The Ring Signature Algorithm was employed. Any user in a group of users who have keys can perform a Ring Signature, a type of digital signature. As a result, a communication bearing a ring signature signifies the endorsement of a certain group of individuals. A ring signature's computational impossibility to identify which member key of the set was utilized to create the signature is one of its security features. Similar to group signatures, ring signatures have two main differences: any group of users can be used as a signing set without further setup, and an individual's anonymity cannot be revoked.

CONCLUSION AND FUTURE SCOPE

Since block chain technology provides a novel approach to data distribution and storage that is both safe and traceable, it has taken the industry by storm in recent years. The block chain actually actively helps to preserve network users' anonymity and the security of their personal data. However, block chain has some security flaws, such as DoS, eclipse, and double spending attacks. To solve the current problems, advanced anomaly detection and mitigation approaches—that is, techniques utilising AI algorithms—are essential. The primary goal of the discussed integration of artificial intelligence and block chain technology is to create a safe, dependable, and effective block chain network for smart environments. We focused our research on how AI might help block chain networks in terms of enhancing security and protecting privacy in block chain-based smart environments.

The methodology it provided grouped the block chain security challenges—financial gain, de-anonymization, and isolation attacks—according to the attacker's aim. It displays the abilities of BT-AI integration, encompassing privacy preservation, anomaly detection, and transaction classification. Regarding the BT-AI ideals, we talked about how to strengthen security and privacy while also enhancing scalability and cyber resilience. Not to mention, they talked about a few pertinent research topics that could result in fascinating new fields of study, such the online learning model for cyber resilience, the BT-AI from a data-oriented perspective, and the decentralized content provider for privacy preservation.

FUTURE SCOPE

Examine methods to enhance the scalability and performance of block chain-based systems in light of the growing amount and speed of Internet of Things data. Examine ways to optimize homomorphic encryption to minimize reduce computational burden and improve effectiveness without sacrificing security. Create AI models and algorithms especially for resource-constrained IoT devices to enhance their functionality and reduce energy usage. Examine how federated learning approaches can be used with block chain technology and homomorphic encryption to allow for cooperative, private AI model training across a variety of Internet of Things devices. Investigate cutting-edge differential privacy techniques that can protect data privacy and allow for insightful analysis and artificial intelligence. Big data applications have drawn increasing attention to distributed data-sharing systems. Our next research focus will be on anonymous authentication and key distribution in the Internet of Things data-sharing system.

REFERENCES :

[1] D. Huang, X. Ma, and S. Zhang, “Performance analysis of the raftconsensus algorithm for private blockchains,” IEEE Trans. Syst., Man, Cybern., Syst., vol. 50, no. 1, pp. 172–181, Jan. 2020, doi: 10.1109/TSMC.2019.2895471.

[2] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, “An identity management and authentication scheme based on redactableblockchain for mobile networks,” IEEE Trans.Veh. Technol., vol. 69, no. 6, pp. 6688–6698, Jun. 2020.

[3] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, “Edge-assisted privacypreserving raw data sharing framework for connected autonomous vehicles,” IEEE Wireless Commun., vol. 27, no. 3, pp. 24–30, Jun. 2020, doi: 10.1109/MWC.001.1900463.

[4] X. Luo, K. Xue, J. Xu, Q. Sun, and Y. Zhang, “Blockchain based secure data aggregation and distributed power dispatching for microgrids,”IEEE Trans. Smart Grid, vol. 12, no. 6, pp. 5268–5279, Nov. 2021.

[5] K. Fan, T. Liu, K. Zhang, H. Li, and Y. Yang, “A secure and efficient outsourced computation on data sharing schemefor privacy computing,”J. Parallel Distrib. Comput., vol. 135, pp. 169–176, Jan. 2020.

[6] F. Jamil, N. Iqbal, Imran, S. Ahmad, and D. Kim, “Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid,”

[7] Z. Shahbazi and Y.-C. Byun, “Integration of blockchain, iot and machine learning for multistage quality control and enhancing security in smart manufacturing,”

[8] Kumari, R. Gupta, S. Tanwar, and N. Kumar, “Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions,”