International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

PRIVACY PRESERVING IN IOT WHILE DATA SHARING BASED ON BLOCKCHAIN

B. Shanmuga Sundari[1], M. Janaki[2]
[1]Assistant Professor, Department of CSE, PET Engineering College, Vallioor
[3]PG Student, Department of CSE, PET Engineering College, Vallioor

ABSTRACT

The proliferation of Internet of Things (IoT) devices has led to an unprecedented generation of data, presenting significant oppounities for innovation and efficiency. However, the sharing of sensitive IoT data raises substantial privacy concerns. The novel approach to privacy-preserving IoT data sharing using blockchain technology. Smart contracts are employed to define and enforce access control policies, ensuring that only authorized parties can access specific IoT data. The approach eliminates the need for a centralized authority, enhancing privacy. Cloud-based storage services have been the dominating outsourcing solution for both individuals and organizations to share data digitally. Despite the advantages, users must rely on storage services for data confidentiality, data access control, user privacy, and data availability. Whereas data confidentiality can be protected by advanced encryption algorithms, the rest remain challenging. Third, a huge amount of data is daily generated and stored on a centralized party, simultaneously serving requests from many users, which may cause a collapse of the system during peak periods. To address all these concerns, we propose a privacy-preserving blockchain-based data sharing platform for the Inter Planetary File System (IPFS), a content-addressable peer-to-peer storage system

Keywords-privacy preserving,smart contracts,Encryption Alogorithms.

I. INTRODUCTION

The widespread attention and application of artificial intelligence (AI) and blockchain technologies, privacy protection techniques arising from their integration are of notable significance. In addition to protecting privacy of individuals, these techniques also guarantee security and dependability of data. It initially presents an overview of AI and blockchain, summarizing their combination along with derived privacy protection technologies.

This chapter discusses a software-defined network-based framework[1]. for future smart cities. In the proposed addressing scheme, a new Internet of Things (IoT) device will receive an internet protocol address from one of their existing neighbouring peer devices. Manual configuration of IoT devices in most of the cases is inapplicable and error prone due to large size of the network.

In the Internet of Things (IoT) scenario, the block-chain and, in general, Peer-to-Peer approaches[2] could play an important role in the development of decentralized and data intensive applications running on billion of devices, preserving the privacy of the users. Our research goal is to understand whether the blockchain and Peer-to-Peer approaches can be employed to foster a decentralized and private-by-design IoT.

As a first step in our research process, we conducted a Systematic Literature Review on the blockchain to gather knowledge on the current uses of this technology and to document its current degree of integrity, anonymity and adaptability.

Blockchains allow us to have a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner[3]. We review how this mechanism works and also look into smart contracts-scripts that reside on the blockchain that allow for automation of multi-step processes.

Internet of Things (IoT) vision, conventional devices become smart and autonomous. This vision is turning into a reality thanks to advances in technology, but there are still challenges to address, particularly in the security domain e.g., data reliability [4].

Blockchain technology has been transforming the financial industry and has created a new crypto-economy in the last decade. The foundational concepts[5]. such as decentralized trust and distributed ledger are promising for distributed, and large-scale Internet of Things (IoT) applications.

II. LITERATURE SURVEY

In 2008 A. Panarello Published his study on The Internet of Things (IoT) refers to the interconnection of smart devices to collect data and make intelligent decisions[6]. However, a lack of intrinsic security measures makes IoT vulnerable to privacy and security threats This paper presents the following novelties, with respect to related work: (i) it covers different application domains, organizing the available literature according to this categorization, (ii) it introduces two usage patterns, i.e., device manipulation and data management (open marketplace solution), and (iii) it reports on the development level of some of the presented solutions.

In 2018 T.M. Fernandez-Carames The paradigm of Internet of Things (IoT) is paving the way for a world, where many of our daily objects will be interconnected and will interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment, and self-maintenance. Such features can be brought by blockchain, a technology born with a cryptocurrency called Bitcoin.[7].

In 2018 M. Banerjee nternet of Things (IoT) devices are increasingly being found in civilian and military contexts, ranging from smart cities and smart grids to Internet-of-Medical-Things, Internet-of-Vehicles, Internet-of-Military-Things, Internet-of-Battlefield-Things, etc. In this paper, we survey articles presenting IoT security solutions published in English since January 2016. We make a number of observations, including the lack of publicly available IoT datasets that can be used by the research and practitioner communities[8].

In 2018 H. F. Atlam The Internet of Things (IoT) has extended the internet connectivity to reach not just computers and humans, but most of our environment things[9]. The IoT has the potential to connect billions of objects simultaneously which has the impact of improving information sharing needs that result in improving our life.

In 2018 Z. Zheng Blockchain has numerous benefits such as decentralization, persistency, anonymity and auditability[10]. There is a wide spectrum of blockchain applications ranging from cryptocurrency, financial services, risk management, Internet of Things to public and social services. Although a number of studies focus on using the blockchain technology in various application aspects, there is no comprehensive survey on the blockchain technology in both technological and application perspectives.

III. EXISTING SYSTEM

These are the physical devices that collect data from various sources in the IoT ecosystem. Examples include sensors, smart devices, and connected machines. These entities gather data from IoT devices and transmit it securely to the system for further processing. They ensure the integrity and authenticity of the data. The collected data from IoT devices is transmitted securely to the system, ensuring privacy and security.

The IoT data is encrypted using homomorphic encryption techniques. The encryption method allows computations to be performed on the encrypted data without the need to decrypt it. The encrypted IoT data is stored on a blockchain, which provides immutability, transparency, and decentralization. The blockchain ensures the integrity and security of the data, making it tamper-proof.

Disadvantages Of Existing System

One of the main disadvantages of blockchain technology is the **immutability of data**.

While blockchain technology provides immutability and transparency, the security of the blockchain itself is crucial. Vulnerabilities or attacks targeting the blockchain infrastructure can compromise the integrity and confidentiality of the shared IoT data. Ensuring the robustness and security of the blockchain implementation, including secure consensus mechanisms and protection against potential threats, is of paramount importance.

IV. PROPOSED SYSTEM

These are the physical devices in the IoT ecosystem that collect data from various sources. Examples include sensors, smart devices, and connected machines. The IoT devices collect data and encrypt it using homomorphic encryption techniques.

Advantages of Proposed System

 Public key is received from the server.

 Handshake is made to the server using that public key.

 Data is transferred to the server in the encrypted using the token.

 The data CRC is checked and acknowledgment and reward is returned.

V. SYSTEM ARCHITECTURE

This technology uses certain cryptographic algorithms to verify data and record transactions send to peers in block. Each new verified block uses cryptographic hash functions to form an immutable, traceable blockchain network. Transactions on the chain are immutable, and it is impossible to change them mathematically.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

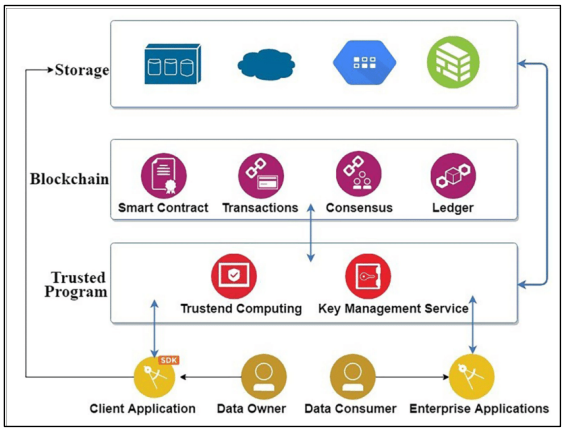

Fig 5.1 System Architecture

VI. SYSTEM IMPLEMENTATION

6.1 MODULES

1. Signup
2. Sign-in
3. UUID verification module
4. Transaction Module
5. Malicious Cloud User identification
6. Verification and Rewarding

6.2 MODULE DESCRIPTION

6.2.1 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

6.2.2 SIGN-IN

- Any registered user who wish to perform a transaction in the blockchain network must login each time to get their identification details like UUID and tokens
- An optional 2 factor authentication could be used for enhanced safety
- Login verification is securely processed with OAuth2.0 token.
- All details like date, time, IP address are stored each time when a user performs login

6.2.3 UUID VERIFICATION MODULE

- UUID stands for Unique User Id
- Each user is assigned with a UUID which is absolutely unique. This UUID changes over a period of time for added security.
- In order to verify the authenticity of each request the UUID is verified constantly.
- If in case the UUID doesn't matches, the transaction request would be cancelled immediately
- If the algorithm finds anything suspicious, the UUID is regenerated and the verification process is done again.

6.2.4 TRANSACTION MODULE

- After the UUID and OAuth2 verification, the file uploading process is initiated and processed.
- Checksum verification is performed in the file before performing the transaction.
- After successfully uploading the file to the server, a token id is returned which will be verified against the rewarding system

6.2.5 MALICIOUS CLOUD USER IDENTIFICATION

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

- 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.

6.2.6 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
- Once the rewarding is successful, the system resets UUID, tokens and OAUTH 2.0 tokens

VII. RESULTS AND DISCUSSION

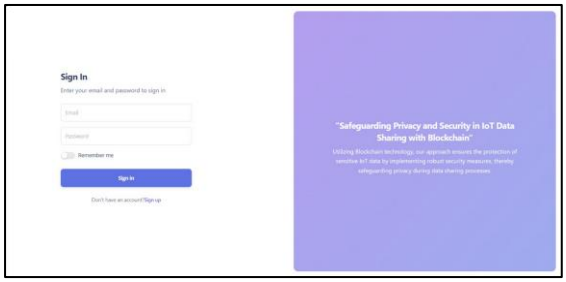

Fig 7.1 sign in Page

This is where users enter their unique identifier, which may be a username, email address, or another piece of information associated with their account. Users input their secret password in this field, serving as a second factor for authentication. Passwords are typically hidden to protect them from being visible. After entering the required credentials, users click the "Sign-In" or "Log In" button to submit their information and initiate the authentication process.

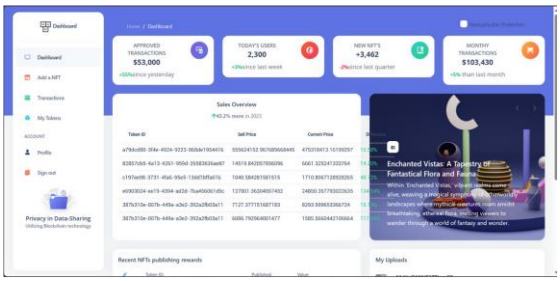

Fig 7.2 Dashboard site

Users often have the ability to customize dashboards to suit their specific needs and preferences. This may include selecting the KPIs to display, arranging visual elements, and adjusting settings for a personalized experience. Many dashboards support interactivity, enabling users to drill down into specific data points, filter information based on criteria, or toggle between different views. Interactive elements enhance the user's ability to explore and analyze data.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

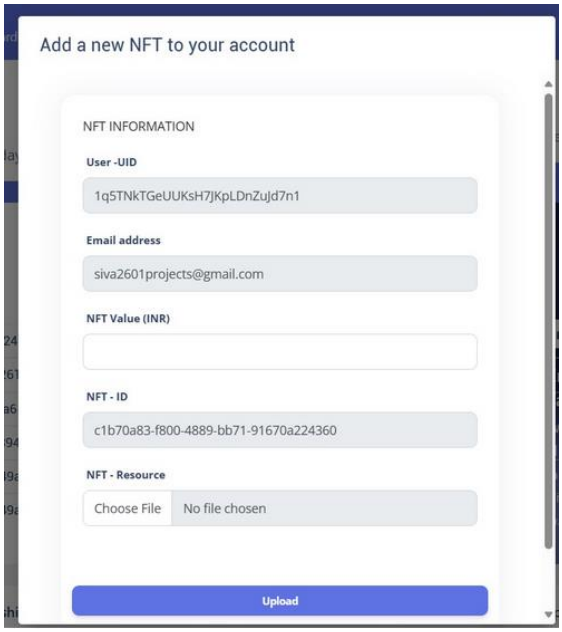

Fig 7.3 Add a New NFT

If you don't have an account on the chosen platform, you'll need to create one. This usually involves providing an email address, creating a password, and sometimes completing a KYC (Know Your Customer) process. Most NFT platforms require you to have a cryptocurrency wallet to store your NFTs. Your wallet address is where the NFTs will be sent. If you don't have a wallet, create one on the platform or use a compatible external wallet.

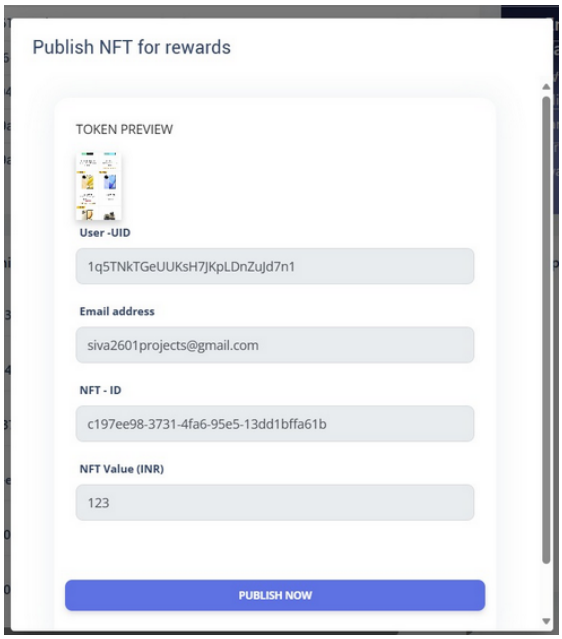

Fig 7.4 Publish NFT for Rewards

Choose a blockchain platform that supports NFTs. Ethereum, Finance Smart Chain, and Flow are examples of popular blockchains for NFTs. If you don't have a cryptocurrency wallet, create one. This wallet will be used to store your NFTs. Ensure that it is compatible with the blockchain platform you've chosen. Choose a minting platform or marketplace where you can create and publish your NFT. Platforms like Open Sea (for Ethereum), Rarible, or Mintable offer minting services. Connect your wallet to the chosen platform.

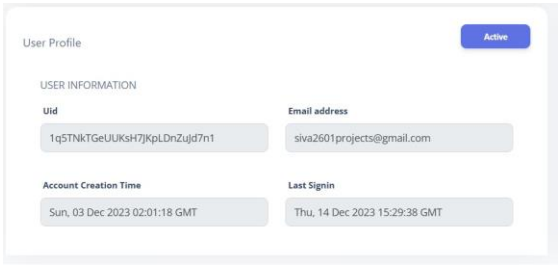

Fig 7.5 User Profile

A record of the user's interactions, activities, and history within the system. This may include posts, comments, transactions, or other relevant actions. Information about the user's connections or relationships within the platform, such as friends, followers, or contacts. Some platforms display a list of connections on a user's profile.

Fig 7.6 Transaction

In the context of blockchain technology, a transaction represents a record of the transfer of assets (such as cryptocurrency) from one participant to another. Blockchain transactions are often decentralized, secure, and immutable.

VIII. CONCLUSION AND FUTURE ENHANCEMENTS

Blockchain technology has invaded the industry sector in past years since it provides a unique approach for storing and transmitting data in a traceable and secure manner. In fact,the blockchain plays an active role in securing users' data and maintaining network members' anonymity. However, blockchain presents some security concerns namely DoS, eclipse, and double spending attacks. For existing challenges to be overcome, advanced anomaly detection and mitigation techniques, more precisely those utilizing AI algorithms, are essential. The addressed the incorporation of blockchain technology and artificial intelligence which the main purpose is to provide a secure reliable, efficient blockchain network for smart environments. It narrowed our research to study how AI can assist blockchain networks; in terms of security improvement and privacy preserving in blockchain based smart environments. We started by detailing the taxonomy of both technologies AI and BT, we introduced its architecture, protocols and functionalities as well as its areas of deployment (smarts environ ments).

It proposed framework presented the blockchain security challenges that are categorized based on the attacker's intention namely financial gain, de-anonymization, and isolation attacks. Itpresents the capabilities of BT-AI integration, which include transaction classification, anomaly detection, and privacy preservation. As for the BT-AI values, we discussed the improvement of scalability and cyber resilience, as well as the enhancement of security and privacy. Last but not least, They discussed some relevant research trends that might lead to interesting research areas such as the decentralized content provider for privacy preservation, the BT-AI for a data-oriented perspective and the online learning model for cyber resilience.

REFERENCES

[1] Tian Li,Huaqun wang,Debiao He, Blockchain Based Privacy Preserving and Rewarding Private Data Sharing For Iot

[2] Bernish Sharana M, Shanmuga Sundari B, Baburengarajan S, Blockchain Technology for Secure Supply Chain Management, International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET) , e-ISSN: 2319-8753, p-ISSN: 2347-6710
.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[4] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173 – 190, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17329205

[5] G. S. Ramachandran and B. Krishnamachari, "Blockchain for the IoT: Opportunities and challenges," CoRR, vol. abs/1805.02818, 2018. [Online]. Available: http://arxiv.org/abs/1805.02818

[6] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," Sensors, vol. 18, no. 8, 2018. [Online]. Available: https://www.mdpi.com/1424-8220/18/8/2575

[7] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," IEEE Access, vol. 6, pp. 32 979– 33 001, 2018.

[8] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," Digital Communications and Networks, vol. 4, no. 3, pp. 149 – 160, 2018. [Online]. Available:

http://www.sciencedirect.com/science/article/pii/S2352864817302900

[9] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," International Journal of Intelligent Systems and Applications, vol. 10, no. 6, pp. 40–48, June 2018. [Online]. Available:
https://eprints.soton.ac.uk/421529/

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[11] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A com- prehensive survey," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1676–1717, Secondquarter 2019.

[12] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," CoRR, vol. abs/1906.00245, 2019. [Online]. Available: http://arxiv.org/abs/1906.00245

[13] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp.2188–2204, 2019.

[14] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in iot: The challenges, and a way forward," Journal of Network and Computer Applications, vol. 125, pp. 251 – 279,2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804518303473

[15] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," IEEE Access,vol. 7, pp. 10 127–10 149, 2019.

[16] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and chal-

lenges," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1508–1532, 2019.

[17] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture,

consensus, and traffic modeling," ACM Comput. Surv., vol. 53, no. 1, Feb. 2020. [Online]. Available: https://doi.org/10.1145/3372136

[18] T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," IEEE Access, vol. 8, pp. 9146–9156, 2020.

[19] W. LI, W. MENG, Z. LIU, and M.-H. AU, "Towards blockchain-based software-defined networking: Security challenges and solutions," IEICE Transactions on Information and Systems, vol. E103.D, no. 2, pp. 196– 203, 2020.

[20] C. Luo, L. Xu, D. Li, and W. Wu, "Edge computing integrated with blockchain technologies," in Complexity and Approximation: In Memory of Ker-I Ko, D.-Z. Du and J. Wang, Eds. Cham: Springer International Publishing, 2020, pp. 268–288. [Online]. Available: https://doi.org/10.1007/978-3-030-41672-0_17