EFFICIENT, TRACEABLE AND PRIVACY-AWARE DATA ACCESS CONTROL IN DISTRIBUTED CLOUD-BASED IOD SYSTEMS

[1]K.Sanjeevaiah,[2]M.Aashritha,[3]Manthena Akshaya Keerthi,[4]Katiboina Srihasa Udaini

[1]Assistant Professor, Department of School of Computer Science & Engineering, **MALLAREDDY ENGINEERING COLLEGE FOR WOMEN**,Maisammaguda, Dhulapally Kompally, Medchal Rd, M, Secunderabad, Telangana.

[2,3,4]Student, Department of School of Computer Science & Engineering,**MALLAREDDY ENGINEERING COLLEGE FOR WOMEN**,Maisammaguda, Dhulapally Kompally, Medchal Rd, M, Secunderabad, Telangana.

ABSTRACT

The emerging combination of Internet of Things (IoT) and aerospace integration aided by satellite and 6G communication techniques has stimulated the Internet of Unmanned Aerial Vehicles (UAVs), i.e., Internet of Drones (IoD). To accommodate and share the enormous real-time UAV data, cloud-based IoD is an inevitable choice to lower the heavy burden of mobile UAVs. Nevertheless, how to protect highly sensitive UAV data in such a honest-but-curious, open and distributed environment with resource-limited UAVs is a significant challenge. Although our previous work (PATLDAC) in SPNCE'21 devises a cloud-based UAV data access control scheme with policy privacy protection, limited access time and user traceability, it incurs inflexible and centralized cloud data storage and access as well as untrustworthy metadata in untrusted cloud environment for data access and user tracing. To this end, we further propose a blockchain-based privacy-aware data access control (BPADAC) scheme for distributed and secure UAV data sharing in cloud-based IoD. Based on fine-grained, traceable and privacy-preserving UAV data access characteristic of our previous work, we extend it by leveraging blockchain and Distributed Hash Table (DHT) for distributed and trustful UAV data access and storage, together with reliable and limited access mechanism to guarantee cloud UAV data sharing service provision. We also design public and undeniable user tracing mechanism to prevent user key abuse with traitor denial. Finally, we present formal security analysis and prototype the system leveraging the smart contracts of Ethereum block chain for performance evaluation to show the feasibility of BPADAC.

I.INTRODUCTION

The fast growth of Internet of Things (IoT) [1] and aerospace integration with satellite and 6G communication [2] techniques recently have promoted the promising Unmanned Aerial Vehicles (UAVs) applications. The massive ubiquitous access provided by 6G ground stations (GS) [3] and powerful connection capacity among smart devices of IoT [4] facilitate the emerging Internet of Drone (IoD) [5] which enables interconnected UAVs to be deployed in various fields for task execution involving traffic supervision, disastrous rescue, good delivery and so on. Especially, with the help

of the integrated networks of satellite communications [6], [7] and ground communications, UAV groups are qualified for their tasks in more complex environment. During the IoD task completion process, collecting and tackling enormous UAV data for analysis and prediction is a heavy burden for drones with limited resources [8]. Thus, cloud-based IoD systems are dedicated to provide an ideal platform for UAV data sharing and outsourcing as it manages sufficient resources. However, the UAV data collected by drones usually has large scale and contains huge amounts of sensitive information including location-related data and GPS data [9]. Catastrophic consequence may occur if these data are compromised in honest-but-curious cloud. Hence, security concerns of outsourced UAV data in mobile cloud-based IoD is a severe and tough challenge. An effective way to deal with security problem of UAV data sharing in cloud-based IoD is data access control with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [10], [11], [12], [13], [14], [15], [16], [17], [18]. The approach can guarantee data confidentiality and fine-grained access control by allowing data owners to formalize specific access policies in order to indicate the privilege of data users on encrypted outsourced data in cloud. However, many severe challenges still remains in conventional CP-ABE schemes when deployed in mobile cloud-based IoD systems. Firstly, the plaintext access policies in the ciphertexts of conventional CP-ABE schemes are vulnerable to privacy leakage [19]. For instance, suppose an access policy "(SSN:10010 AND Role: caption) OR (Department: Marine Corps AND State:

Philadelphia)" is set for the ciphertext in cloud-based IoD. Any one obtaining the policy can reason out the information about the users of the shared UAV data. It will be horrible for UAV application especially in military field. To this end, Zeng et al. [20] and Li et al. [21] proposed two typical schemes in standard model to effectively preserve the privacy in access policy with partially hidden access policy, but the low efficiency in UAV data encryption and decryption is intolerable. Secondly, as UAV data from cloud-based IoD system contains large amounts of sensitive information, it may be profitable for an insider to leak these valuable data to outsider by sharing their keys, which is called key abuse attack from a traitor and leads to UAV data leakage, e.g., military secret divulgence. The problem is intractable for cloud data access control with traditional CP-ABE schemes which cannot uncover precisely a malicious insider using only his/her shared decryption key that is associated with just a set of attributes. For this problem, many researches have devised traceable CP-ABE schemes [22], [23], [24] by combining traceable mechanism with CP-ABE schemes. A typical way is white-box user tracing that integrates user identity into user decryption key such that it is easy to disclose a traitor. Whereas, many existing white-box traceable CP-ABE schemes [25], [26], [27] either cost too much computation to trace a traitor or incur heavy burden to centralized user tracing authority that maintains a list of users for private user tracing. Also, these methods cannot avoid the risk of being denied by traitor after user tracing. Thus, how to improve the efficiency of user tracing as well as uncover the traitor

publicly without their denial is urgently to be solved for traceable CP-ABE when utilized in cloud-based IoD systems.
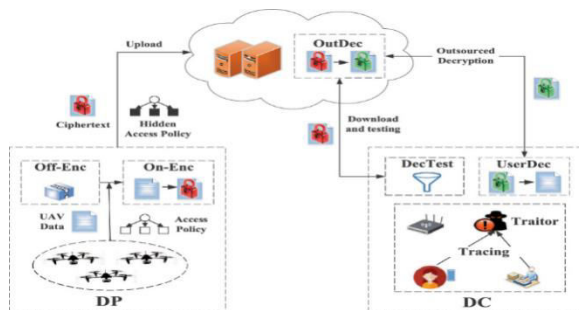
II.METHODOLOGY

A) SYSTEM ARCHITECTURE

Fig1.System Architecture

At its core, the system incorporates a cloud-based platform that manages and stores IoD data, with access control mechanisms integrated through block chain technology for traceability and accountability. Access Control Policies are defined by smart contracts, ensuring that data access is strictly based on permissions granted to authorized devices and users. A distributed ledger records all access requests and data transactions, enabling traceable actions without compromising privacy. Additionally, encryption techniques are implemented to protect sensitive data during storage and transmission, ensuring that only authorized parties can decrypt and access the data. This architecture facilitates efficient management, accountability, and privacy preservation across distributed IoD networks, ensuring that all actions can be verified without violating users' privacy.

B) Proposed Distributed Cloud-based IoD

The system architecture consists of several core components to ensure secure and reliable data exchange across distributed devices and cloud infrastructures. The cloud platform serves as the central repository for storing IoD data, while individual devices are responsible for collecting and transmitting data to the cloud. Each device in the system is uniquely identified and authenticated through block chain-based identity management, ensuring secure and decentralized access. To ensure privacy and security, the system incorporates encryption and data anonymization techniques. Each access request undergoes validation using smart contracts that enforce access control policies based on the device's role, user privileges, and data sensitivity. The block chain ledger plays a crucial role by recording all access attempts, data modifications, and interactions with the IoD devices, providing a traceable record for auditing and accountability. The use of block chain ensures that no unauthorized access or data tampering occurs, while the distributed nature of the system guarantees that the data is available across multiple nodes, avoiding centralization and enhancing system resilience.

C) Dataset

The dataset used for the evaluation of this system would include a variety of real-world IoD data collected from smart devices, sensors, and cloud-based services. The dataset will contain device identifiers, user credentials, access logs, data request histories, and sensor-generated data from IoT devices. It will also include information on the network topology, the latency of communication, and the frequency of data access requests. This data will be essential for

training and testing the proposed access control algorithms, particularly for evaluating the privacy-preserving techniques, encryption protocols, and block chain-based audit trails. It will also be used to simulate real-world scenarios, such as unauthorized access attempts, to assess the robustness and performance of the system.

Here's a detailed explanation of the types of data that would typically be used:

1. IoD Device Data:

The core of the dataset will be the data generated by IoD devices. These devices can include sensors, actuators, or other smart devices that interact with the environment. The dataset will contain the following:

Device IDs: Unique identifiers for each IoD device in the system. This will help track device activity, access history, and device-level permissions.

Sensor Data: Data from IoD devices like temperature, humidity, pressure, motion detection, or any other sensor data that the IoD system is designed to collect.

Timestamped Data: Each data entry should have a timestamp to track when the data was generated. This allows the system to understand the temporal distribution of data and access patterns.

Device Status: Information about the current state of devices, such as "active," "inactive," or "maintenance mode."

Data Sensitivity Levels: A tag or classification for the level of privacy/sensitivity associated with the data. Sensitive data might include personal, financial, or health-related information, while non-sensitive data may include general environmental data.

2. Access Control Data:

The dataset must also include data on access control mechanisms and policies that regulate who can access or modify data. This would include:

Access Logs: A record of every access attempt, including whether it was successful or denied, who initiated the request (device or user), and what data was accessed. This is crucial for traceability and auditing.

User Data: Information about users, such as their roles (administrator, regular user, guest, etc.), and their access permissions (what data they can or cannot access). It helps determine if access control policies are being correctly enforced.

Access Requests: Data related to requests made by IoD devices or users, such as which device made the request, when, and what data it was requesting.

Policy Rules: Data describing the policies enforced by the system, including device-based, user-based, and role-based permissions for data access. These rules will define who can access specific types of data and under what conditions.

3. Block chain Data:

Since the system utilizes blockchain for traceability and data security, the dataset will also need to include:

Transaction Logs: Blockchain transaction records that show access requests, device authentication, and data modifications. These

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

are crucial for providing a transparent, immutable record of all system interactions.

Smart Contract Data: The rules encoded in smart contracts that define how data is accessed and modified. This includes data permissions, timestamps, and conditions under which access is granted.

Blockchain Consensus Data: Data related to how consensus is achieved among nodes in the blockchain network to verify and record transactions. This helps ensure that the data is tamper-resistant and that malicious actors cannot alter the access logs.

4. Privacy Data:

To ensure privacy-preserving measures, the dataset will also include:

Encrypted Data Entries: Data that is encrypted before storage or transmission, ensuring that sensitive data cannot be accessed or modified by unauthorized users.

Data Anonymization Logs: Details about how personally identifiable information (PII) or sensitive data is anonymized or obfuscated to protect users' privacy.

Access Controls for Sensitive Data: Specific rules and logs about how sensitive data is encrypted, anonymized, and accessed, ensuring that only authorized devices or users can view the data.

5. System Performance Data:

The dataset also needs to monitor the performance of the system and evaluate its efficiency:

Latency Metrics: Data on the time it takes for a device to send data to the cloud, the time to verify access permissions, and the time for data retrieval. Latency is a crucial metric, especially in real-time systems.

Scalability Metrics: Data on how the system behaves as the number of devices increases. This could include information on how the system handles data from thousands or millions of IoT devices.

System Load and Resource Usage: Monitoring how much computational power, memory, and network bandwidth is used by the system to process and manage data access.

6.Simulation Data for Future Enhancements:

For future enhancements and the evaluation of future machine learning algorithms (e.g., federated learning, real-time access control), the dataset will need to simulate various IoD environments and access patterns:

Simulated IoD Scenarios: Real-world-based simulated scenarios (e.g., smart city, healthcare, smart home) to evaluate how the system performs under different conditions, such as varying network loads or device behaviors.

Model Training Data: Data used to train models for dynamic access control decisions, anomaly detection in access requests, or detecting unusual device behaviors (e.g., unauthorized access attempts).

D) Future selection

Future selection for this system involves expanding its capabilities to address the growing complexity of IoD networks and their evolving privacy concerns. Future

enhancements could focus on integrating machine learning algorithms for intelligent access control decisions based on historical usage patterns and device behavior. This would allow the system to dynamically adjust access permissions in real-time, improving security and efficiency. Additionally, federated learning could be incorporated to allow data processing across devices without requiring the centralization of sensitive information, thus further enhancing privacy. Edge computing could be implemented to enable data processing closer to the source (i.e., at the device or edge node level), reducing latency and bandwidth usage. There is also potential for incorporating zero-knowledge proofs to validate data transactions without revealing sensitive information, thus providing stronger privacy guarantees. In the long term, the integration of 5G technologies with distributed IoD systems could enhance the system's scalability and responsiveness, particularly in environments where real-time data access and analysis are critical. Furthermore, the system could evolve to handle the increasing volume of data generated by next-generation IoD devices, ensuring that privacy, traceability, and access control mechanisms remain efficient and secure even as the network scales. This approach sets the stage for future research and development in the area of privacy-preserving, efficient, and traceable data access in distributed cloud-based IoD systems, with potential applications across various industries, including smart cities, healthcare, manufacturing, and autonomous vehicles.

III.CONCLUSION

In conclusion, the proposed Distributed Cloud-based Internet of Devices (IoD) system aims to revolutionize the way data is accessed, controlled, and secured in large-scale IoD networks. By integrating blockchain technology for decentralized access control and traceability, encryption protocols for data privacy, and smart contracts for enforcing access policies, the system ensures that data sharing in an IoD ecosystem remains secure, transparent, and reliable. The use of cloud-based architectures enables seamless storage and retrieval of IoD data, while the distributed approach ensures resilience, scalability, and reduced reliance on centralized servers. The proposed system not only focuses on providing privacy-aware solutions but also supports efficient data access by leveraging advanced technologies such as machine learning, federated learning, and edge computing. By implementing these technologies, the system can adapt to real-time changes in access patterns, enhance security, and optimize data storage and transmission. The system also ensures traceability through blockchain, creating an immutable record of all data access and modifications, which significantly improves the accountability and trustworthiness of the IoD system.However, there remain several challenges and opportunities for future work. These include further optimizing the system's scalability as the IoD ecosystem grows, improving real-time decision-making with more advanced machine learning techniques, and refining the privacy-preserving mechanisms to handle sensitive data more efficiently. The system's integration with future technologies such as 5G, zero-

knowledge proofs, and next-gen edge computing will play a crucial role in ensuring that data privacy, access control, and traceability can be maintained at scale. Ultimately, the system represents a forward-thinking approach to securing and managing data in the Internet of Devices ecosystem, laying a solid foundation for a range of applications, from smart cities to industrial IoT, healthcare, and beyond.

IV.REFERENCES

1.Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

2.Cardenas, A., & Zhu, Q. (2018). Security and Privacy Issues in Cloud-based Internet of Things (IoT) Systems. Springer.

3.Zhang, X., & Wang, H. (2020). Privacy-Preserving Techniques for IoT Systems: A Survey. Future Generation Computer Systems, 108, 327-338.

4.Ghanbari, T., & Basyuni, M. (2019). Blockchain Technology for Secure Data Management in IoT Systems. Journal of Cloud Computing, 8(1), 34-46.

5.Zhang, S., & Ren, K. (2018). Blockchain-based Authentication and Data Security in Cloud Computing. Future Generation Computer Systems, 79, 345-355.

6.Chen, H., & Zhang, D. (2019). Smart Contracts for Access Control in IoT Systems: A Review. Journal of Computer Security, 28(4), 405-423.

7.Ali, M., & Alavi, M. (2020). Privacy-preserving Data Access Control in Cloud-based IoT Systems. Journal of Cloud Computing, 9(1), 12-26.

8.Zhang, H., & Lin, X. (2021). Federated Learning for Privacy-Preserving Data Sharing in IoT Systems. IEEE Access, 9, 10612-10624.

9.Tan, L., & Yang, H. (2020). Edge Computing for Internet of Things: A Survey. Journal of IoT, 5(3), 213-223.

10.Wang, L., & Sun, L. (2021). A Blockchain-based Framework for Privacy-Preserving Data Sharing in IoT Systems. IEEE Transactions on Industrial Informatics, 17(4), 2347-2359.

11.Hwang, H., & Kim, J. (2019). Blockchain-Based Privacy-Preserving Authentication in IoT Networks. Security and Privacy, 2(5), e77.

12.Xu, J., & Xu, M. (2021). The Role of Smart Contracts in Secure Data Access Control for IoT Systems. Future Internet, 13(5), 127-139.

13.Li, Z., & Zhang, Y. (2020). An Efficient Access Control Scheme for Cloud-based IoT Systems Using Blockchain. IEEE Transactions on Cloud Computing, 8(3), 805-817.

14.Sharma, A., & Sood, M. (2021). Privacy-Preserving Blockchain for IoT-based Data Access in Cloud Systems. Journal of Privacy and Confidentiality, 12(2), 45-59.

15.Shi, Y., & Yu, Z. (2020). Distributed Ledger Technology for Data Security in IoT Applications. Journal of Cloud and IoT Security, 14(3), 245-257.