International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Refined and Effective Integration of Access Control Mechanism in Blockchain Enabled DApp

Dr.R.M.R.Shamija Sherryl , M.E., Ph.D.,
Faculty of Computer Science and Engineering , SRM IST Rampuram
Chennai, India
shamijar@srmist.edu.in

Amruthamshu Bhushan G
Computer Science and Engineering SRM Institute of Science and Technology, Ramapuram
Chennai, India
gb3034@srmist.edu.in

Koppula Bharath Kumar
Computer Science and Engineering SRM Institute of Science and Technology, Ramapuram
Chennai, India
bk1913@srmist.edu.in

[3]Kuchukulla Krishi Reddy
Computer Science and Engineering SRM Institute of Science and Technology, Ramapuram
Chennai, India
kk9383@srmist.edu.in

---***---

Abstract -
The combination of the Internet of Things (IoT) and aviation integration with the help of satellite and 6G communication technologies has led to the Internet of Unmanned Aerial Vehicles (UAV) or Internet of Drones (IoD). To host and share large amounts of drone data in real time, cloud-based IoD algorithm Cloudbased IoD is the wrong choice to reduce the weight of mobile drones. However, how to protect the sensitive drone at the fair is a matter of curiosity, and it is very difficult to break the environment where drone use is available and limited resources are available. Although our previous work in SPNCE21 (PATLDAC) developed an air-on middle of the main load of based drone data access control system with privacy policy, limited access time and user tracking, it provides conflicting and centralized cloud data storage for cloud environment and access with unreliable data. It is not reliable in terms of data access and tracking of users. To this end, we propose a blockchainbased privacy data access control (BPADAC) scheme for distributed and secure drone data sharing on cloudbased IoDs. Building on the granular, traceable, and privacypreserving drone data access capabilities of our previous work, we extend this by using blockchain and decentralized hash tables (DHT) to provide secure and reliable wireless access to humanmachine data and storage. as well as reliable and limited access guarantee mechanisms for cloud drone data sharing services. We also set up a public and denial user tracking system to prevent user abuse and deny the traitor. Finally, we propose a prototype for security analysis and performance evaluation using smart contracts on the Ethereum blockchain to demonstrate the feasibility of BPADAC. hash table, attributebased ciphertext encryption policy, and blockchain-based privacy-protected enabled and aware data access control

Key Words: Blockchain, UAV,IoD, Distributed Hash Table, Ciphertext-Policy-Attribute-Based-Encryption, blockchainbased privacy-aware data access control

1.INTRODUCTION

In recent years, the rapid development of the Internet of Things, aviation, and satellite connectivity, and 6G communication technology have promoted the application of unmanned aerial vehicles (UAVs), which are the hope of unmanned vehicles. The global reach provided by 6G ground stations (GS) and the powerful connectivity capabilities of IoT smart devices have supported the advancement of the drone Internet, allowing Drones to connect to various areas to perform vehicle monitoring, disaster relief, rescue, cargo transportation and transportation. Especially thanks to the combination of satellite communication and ground communication, the drone group can operate in different places. When completing the IoD mission, collecting and processing large amounts of UAV data for analysis and prediction is a heavy burden for UAVs with limited resources. Therefore, the cloudbased IoD system aims to provide an ideal platform for UAV data sharing and outsourcing as it manages sufficient resources. However, drone data collected by drones is usually large and contains data related to location, GPS data, etc. It contains a lot of sensitive data, including If this information is honestly but curiously compromised in the cloud, the result could be disastrous. Therefore, the security issue of outsourced drone data is a serious problem in mobile cloudbased IoD. A good way to solve the security problem of drone data sharing in cloudbased Internet of Things is to use ciphertext authority attributebased encryption (CPABE) for data management. Granular access control specifies access rights to show users permission to cloudencrypted external data. However, many serious problems are still encountered when using traditional CPABE solutions in cloudbased radio IoD. First of all, the basic information entered into the ciphertext of the CPABE protocol is always confidential. For example, assume the access code "(SSN: 10010 AND Role: Title) OR (Department: Marine Corps AND State: Philadelphia)" is set as ciphertext on a cloudbased IoD. Anyone with access rights can compile information about a user sharing drone data. This can be dangerous, especially for the use of drones in military operations. For this purpose, Zeng et al. and Lee et al. In the standard model, two solutions are proposed that are effective in protecting the privacy of access rights from some secret access rights, but the ineffectiveness of UAV data encryption and decryption is unacceptable. Second, since drone data from cloudbased IoD systems contains a lot of sensitive information, it can be beneficial for insiders to leak this sensitive information to those outside the shared keys, this is called renegade bug and causes drone information to be cracked, such as leaking military secrets. This problem is a difficult one to solve for cloud data access control using traditional CPABE schemes, which cannot ensure that malicious actors only use the shared decryption key associated with a proce ss. To solve this problem, many studies have combined t he traceability system with CPABE schemes and created a traceable CPABE system. The best way is white box u ser tracking, which integrates the user's identity with the user's decryption key and can easily reveal the traitor. H owever, many existing whitebox traceable CPABE sche mes require too much computation to track down traitors or create a burden on the usercentered monitoring autho rity that manages usernames for user tracking. And none of these methods can prevent the risk of users being reje cted by traitors after being tracked. Therefore, when usin g traceable CPABE in a cloudbased IoD system, how to improve user tracking performance and reveal false trait ors. Traitor rejection is a problem that needs to be solved quickly. In addition, cloudbased IoD systems exist in an open environment and face various attacks from outside , such as reverse attacks, malicious attacks, sniffing and interception, hacking and DoS (denial of service) attacks [28]. Among these attacks, DoS attacks are the most let hal and can prevent data and services from being deliver ed from the cloud to drone users. Bad insiders can acces s shared information, clouding the air and corrupting exi sting information, causing drone data users' requests to b e denied, which can cause serious damage, especially in the military and rescue field. Therefore, data access cont rol in UAV data sharing in cloudbased IoD should consi der this as important. Recently, some existing CPABE s chemes have been proposed to limit data access frequen cy while incurring a large computational cost for access analysis and are not suitable for cloudbased IoD systems with limited UAV resources. In addition, the drone swar m of the IoT system is usually in the mobile phone envir onment and needs to be in a different location from the u sers of the drone data, sharing data storage and access. T herefore, in the face of the scale of big data, how to depl oy a distributed, limited, finegrained IoD system for dro ne data access in a decentralized space is crucial for a cl oud-based IoD system for drone critical information.

2. Body of Paper

The general analysis of the above problems has bro ught serious challenges to UAV data sharing servic es in cloudbased IoD systems. Although our previo us work has introduced a cloudbased drone data acc ess control solution (PATLDAC) with the right to p rivacy, limited access and user tracking, which supp orts data privacy and effective access control, the pr ivacy problem has been solved, but to a certain exte nt, insurgents and significant abusers are the same. occurs at the moment. But it cannot support data tra nsfer speed, and mobile IoD containing a lot of dro ne data especially needs scalability. Additionally, m etadata used for data entry and limited time access poses a serious threat in the cloud, which can lead t o unauthorized access to data entry, especially since it is in the decentralized drone information store. In addition, traitors identified by PATLDAC can also deny their crimes. To solve these issues, this paper presents a blockchainbased privacyaware data acces s control (BPADAC) strategy for distributing and s ecuring drone data in cloudbased IoD. Building on t he granular, traceable, and privacypreserving drone data access features of our previous work, PATLD AC, BPADAC's superior solution protects mobile c loudbased IoD from blockchain connectivity and di stributed hash tables (DHT). taken. one step further. Lower budget. Especially compared with our previ ous work, the conclusions of this paper are as follo ws: Scalable and distributed data storage. There is no longer a need to use centralized cloud in most ex isting solutions and our previous work to accommo date large and growing drone data. Therefore, BPA DAC uses distributed data as well as enabling multi cloud. To ensure its security and reliability, the com bination of blockchain and DHT technology, many clouds of the chain can ensure the ability and trust o f data drone outsourcing. Additionally, like our pre vious PATLDAC project, BPADAC implements th e right of access to protect confidentiality through a partial privacy policy (see Chapter 5 for details). Ø Decentralized, limited and reliable data entry. In a decentralized IoT system, drone data outsourced to decentralized multiple clouds is typically entered de centrally via blockchain for access control and relia bility assurance. To ensure that the drone data shari ng service remains vulnerable to DoS attacks by res tricting access to air traffic, BPADAC can be used by all users by integrating blockchain and limited a ccess to timelimited information, which was not ava ilable in our previous projects. Undeniable, obvious treacherous search, efficiency and security. To solv e the problem of serious abuse, BPADAC was give n the public box free column monitoring system so that every part of the body can be opened and insur gents can be seen without having to maintain userna mes in the root CA. However, to prevent traitors fro m denying evidence of malicious behavior, BPAD AC uses blockchain to accurately record the traitor' s immutable credentials for the exchange. In additio n, through performance evaluation through extensiv e testing and online/offline encryption and outsourc ed decryption testing technology, BPADAC has de monstrated superior performance in data encryption and decryption. We also present the security model and proof of BPADAC, which were not provided i n our previous work.

Scheme	DS	PH	LU	TLDAC	FS	SM	OOE	ODT	VR	PT
Scheme [34]	X	√	X	X	√	√	X	X	X	X
Scheme [35]	X	X	X	X	√	X	√	X	X	X
Scheme [36]	X	X	X	X	X	X	√	X	X	X
Scheme [30]	X	X	√	√	X	X	X	X	X	X
Scheme [37]	X	X	√	X	X	X	X	X	X	√
Scheme [38]	X	X	√	X	X	X	X	X	X	√
Scheme [39]	X	√	X	X	√	√	X	X	X	X
Scheme [19]	X	√	√	X	√	√	X	X	X	X
Scheme [21]	X	√	√	X	X	X	√	X	X	X
Scheme [20]	X	√	√	X	√	√	X	X	X	√
PATLDAC	X	√	√	X	√	√	√	X	√	X
BPADAC	√	√	√	√	√	√	√	√	√	√

Aside from cryptocurrency, the most commonly used blockchain application in various fields is smart contracts. A smart contract is a special protocol that contains a series of logical calculations that are performed in advan ce on the blockchain. Required conditions. It is deployed on a blockchain and the results can self-execute and be verified without human intervention. So a smart contract is actually a type of computer program that makes the blockchain programmable. The r esults of a smart contract are immutable and reliable.

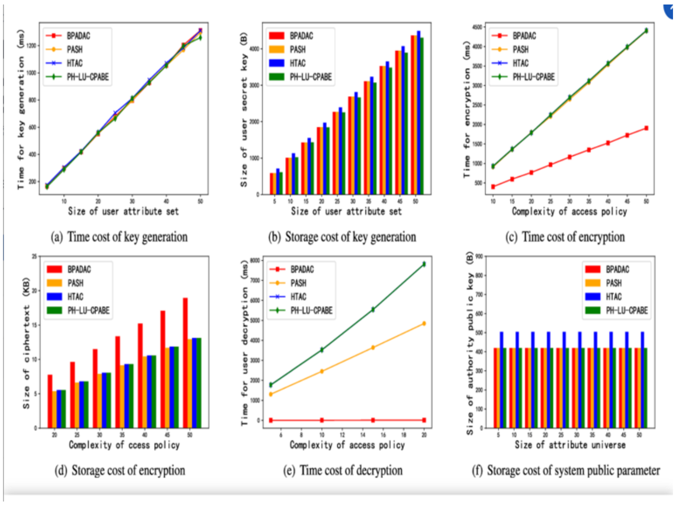
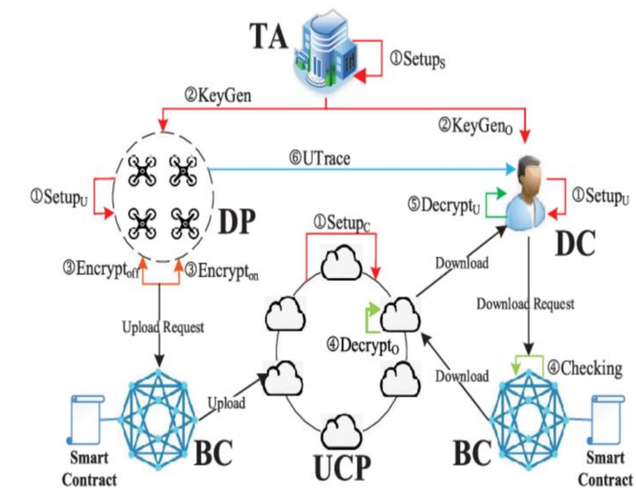


Fig -1: Figure



3. CONCLUSIONS

In this paper, we deeply analyzed the problem of UAV data sharing in cloud IoD systems and then proposed a blockchain-based privacy-aware data access control (BPADAC) method for the equally distributed and secure sharing of the UAV data in mobile and distributed environments. Largescale system. Establishe d a scale environment and provided formal models to support on the every single input type and definitions through detailed configuration. Using blockc hain mechanism to achieve forehand and CP-ABE technology, BPADAC provides granular and decen tralized data for the better understanding and access for authorized data users to access every UAV data via blockchain. At the same time, data exchange ser vices with UAVs can be guaranteed through limited access time mechanisms. Additionally, the combination of multi-cloud and DHT technology can store large-scale UAV data in a distributed and scalable way and overcome the short comings of the mentioned traditional centralized clouds. Partial policy hiding is used in BPDAC to be provide privacy protection for access policies to outsourced the UAV based data in the cloud. Additionally, BPADAC can effectively and openly combat traitor tracking by taking an open approa ch to tracking users without rejection. Additionally, secu rity and performance analysis using a prototype based implemented algorithms based mainly on the Ethereum blockchain provides strong evidence that BPADAC is secure and suitable for UAV communication in cloud-based mechanism similar to our very own IoD systems. Future research will explore the problem of ide ntifying sources of UAV data and outsourced UAV data in cloud-based IoD systems.

ACKNOWLEDGEMENT

I would like to extend my heartfelt gratitude to Ma Zuang and Jiahweh Ziang for their invaluable contributions to provide insight of this project. Their dedication, support, and expertise were essential in refining and integrating the access control mechanism in the blockchain-enabled

DApp. I am deeply thankful for their guidance and collaboration throughout this endeavor.

REFERENCES

[1] X. Li, H. Liu, W. Wang, Y. Zheng, H. Lv, and Z. Lv, ‘‘Big data analysis of the Internet of Things in the digital twins of smart city based on deep learning,’’ Future Gener. Comput. Syst., vol. 128, pp. 167–177, Mar. 2022.

[2] F. Tang, X. Chen, M. Zhao, and N. Kato, ‘‘The roadmap of communication and networking in 6G for the metaverse,’’ IEEE Wireless Commun., early access, Jun. 24, 2022, doi: 10.1109/MWC.019.2100721.

[3] M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywiolek, and I. Ullah, ‘‘Swarm of UAVs for network management in 6G: A technical review,’’ IEEE Trans. Netw. Service Manag., vol. 20, no. 1, pp. 741–761, Mar. 2023.

[4] Z. Na, C. Ji, B. Lin, and N. Zhang, ‘‘Joint optimization of trajectory and resource allocation in secure UAV relaying communications for Internet of Things,’’