Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 737-745)

RESEARCH ARTICLE WWW.PEGEGOG.NET

DATA ACCESS CONTROL FOR CLOUD STORAGE THAT IS SECURE AND EXPRESSIVE

Dr.P.Avinash[1],Ms. Mandula.Akshaya [2], Ms. Ietharaju Rashmini[3], Ms. Repala Thanuja[4]

[1] Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad
avinashcse9294@gmail.com
[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT

Drones, or the Internet of Unmanned Aerial Vehicles (UAVs), have been proliferated by the growing convergence of the Internet of Things (IoT) with aeronautical integration, which has been facilitated by 6G communication technology and satellites. To alleviate the immense workload of mobile UAVs, cloud-based IoD is an essential solution for housing and sharing the massive amounts of real-time UAV data. Yet, a major difficulty is figuring out how to secure critical UAV data in an open, inquisitive, resource-limited, and honest environment. The cloud data storage and access is inflexible and centralized, and the metadata is untrustworthy in an untrusted cloud environment for data access and user tracing. Despite the fact that our prior work (PATLDAC) in SPNCE'21 developed a cloud-based UAV data access control scheme with policy privacy protection, limited access time, and user traceability, these issues still persist. As a follow-up, we suggest a privacy-aware data access control (BPADAC) scheme that uses blockchain technology to facilitate the safe and dispersed exchange of data by UAVs in the context of cloud-based IoD. To build on our earlier work's fine-grained, traceable, and privacy-preserving UAV data access, we use blockchain and Distributed Hash Table (DHT) to store and access UAV data in a distributed and trustworthy manner, and we establish a reliable and limited access mechanism to ensure that UAV data sharing services are provided in the cloud. To avoid user key misuse via traitor denial, we additionally provide a public and unchangeable user tracing system. As a last step in proving BPADAC's viability, we provide formal security analysis and build a prototype that uses Ethereum blockchain smart contracts to measure performance.
Keywords: Distributed Hash Table, Reliable Data, Cloud Computing, Privacy-Preserving, Metadata, UAV Data Control, Centralized Access Control.

1. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) have lately seen a surge in interest due to the rapid expansion of the Internet of Things (IoT) [1] and the integration of satellite and 6G connectivity [2] technology in the aerospace industry. With the advent of the Internet of Things (IoT) and the widespread availability of 6G ground stations (GS) [3], interconnected unmanned aerial vehicles (UAVs) can be used in a variety of contexts to carry out tasks such as traffic monitoring, disaster relief, product delivery, and more.

How to cite this article: M Dr.P.Avinash1,Ms. Mandula.Akshaya 2, Ms. Ietharaju Rashmini3, Ms. Repala Thanuja4. DATA ACCESS CONTROL FOR CLOUD STORAGE THAT IS SECURE AND EXPRESSIVE.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 737-745
Source of support: Nil **Conflicts of Interest:** None.
DOI: 10.48047/pegegog.13.04.81
Received: 12.10.2023
Accepted: 22.11.2023 **Published:** 24.12.2023

In particular, UAV groups are capable of completing their missions in more complicated

environments with the support of integrated networks of ground communications and satellite communications [6, 7]. Drones with limited resources have a tough time gathering and processing massive amounts of UAV data for analysis and prediction throughout the IOD job completion process [8]. It follows that cloud-based IOD systems are devoted to managing enough resources to provide an optimal platform for UAV data sharing and outsourcing. But the data gathered by UAVs is sometimes massive and includes a plethora of sensitive information, such as GPS coordinates and location-related details [9]. If these data are corrupted in the trustworthy but inquisitive cloud, it might have catastrophic consequences. Therefore, there is a significant and difficult difficulty with the security of outsourced UAV data in mobile cloud-based IOD. Data access control using Cipher text-Policy Attribute-Based Encryption (CPABE) is an excellent solution to the security challenge of UAV data sharing in cloud-based IOD [10]. With this method, data owners may formally establish specified access rules that indicate the privilege of data users on encrypted outsourced data in the cloud, guaranteeing data confidentiality and providing for fine-grained access control. Nevertheless, traditional CP-ABE techniques still face several significant obstacles when used in mobile cloud-based IoT systems. To begin, traditional CP-ABE methods leave themselves open to privacy leaks because to their cipher texts' plaintext access restrictions. Consider the following scenario: the encrypted text is stored in cloud-based IOD, and the access policy is configured to "(SSN:10010 AND Role: caption) OR (Department: Marine Corps AND State: Philadelphia)". Anyone with access to the policy may deduce details about the people who used the shared UAV data. Using UAVs, particularly in the military, will be a nightmare. Due to the intolerably poor efficiency in UAV data encryption and decryption, Zeng et al. and Li et al. presented two common approaches in the standard model to successfully protect privacy in access policies with partly concealed policies. Secondly, an insider may find it lucrative to divulge sensitive information from a cloud-based IOD system to an outsider by sharing their keys. This is known as a key abuse attack, and it can lead to the leakage of UAV data, such as military secret divulgence. Using typical CP-ABE systems for cloud data access control is

problematic because it is not possible to identify a malevolent insider based on a shared decryption key and a limited range of qualities. In order to address this issue, several researchers have developed traceable CP-ABE schemes that combine CP-ABE with a traceable mechanism. A common method is white-box user tracing, which makes it easier to expose a traitor by integrating user identification with user decryption key. However, tracking a traitor using several current white-box traceable CP-ABE systems places an undue load on a centralized user tracing authority that keeps track of private user traces, or it requires too much computation. The possibility of denial by a traitor after user tracking is also inherent in these systems. So, for traceable CP-ABE to work in cloud-based IoT systems, we need to figure out how to make user tracking more efficient while also publicly exposing the traitor without their denial. Furthermore, since they are hosted in the cloud, IoT systems are vulnerable to a wide range of external threats, including replay attacks, impersonation attacks, sniffing and intercepting attacks, tampering attacks, Denial of Service (DoS) assaults, and many more. The most devastating of these typical assaults is a denial-of-service (DoS) attack, which may prevent cloud data and service supply to users of unmanned aerial vehicle (UAV) data. In reality, a malevolent insider may persistently access the data sharing system, depleting cloud resources and disrupting data availability. This would lead to the rejection of requests from UAV data consumers, which could have catastrophic consequences, particularly in military field and rescue operations. So, while designing data access control for UAV data sharing in cloud-based IOD systems, this important element should be considered. In order to restrict the frequency of data access, many CP-ABE techniques have been proposed recently. However, these schemes are not appropriate for cloud-based IOD systems that use resource-limited UAV devices since they need expensive computations for access verification. Distributed data storage and access is also necessary since UAV groups of IOD systems are often in a mobile environment and not in the same physical location as UAV data consumers. Consequently, a major concern with UAV data sharing in cloud-based IOD systems is how to implement decentralized environments with dispersed, restricted, and fine-grained UAV data access in the face of huge data size. The significance of data assets in unmanned aerial vehicle (UAV) applications for analysis and prediction has been extensively investigated. The need to protect UAV data is growing as a category of very valuable assets. In order to ensure the safety of communication between unmanned aerial vehicles (UAVs), Tsao et al. [8] suggests a method for secure UAV transmission. Additionally, in order to detect end-to-end communication between UAVs and base stations, Alladi creates an authentication mechanism that is exclusive to UAVs. In addition, Mehta et al. plans to use a

5G-enabled UAV system in conjunction with blockchain technology to safeguard UAV networks. The difficult data access control issue for UAV data sharing in cloud-based IoD systems, however, renders these suggestions useless. To provide data confidentiality and fine-grained access control, CP-ABE has gained widespread acceptance in the data access control research area. It is used in a variety of scenarios involving honest-but-curious public data storage, including cloud data sharing. Despite CP-ABE's usefulness and effectiveness in data security, many applications still find its substantial processing cost in encryption and decryption to be unattractive. Here, Hohenberger and Waters were the first to suggest an online/offline CPABE system, which combined an online/offline computing technique with CP-ABE. The OOMA-CP-ABE system, developed by Xue et al. for use in multi-authority CP-ABE, is the progenitor of the proposed online/offline CP-ABE technique. Many recent research in CP-ABE incorporate the concept of outsourced decryption, which was originally established by Green et al. to mitigate computing costs in decryption. Using this effective paradigm, Lai et al. developed a verifiable outsourced CP-ABE technique to check the accuracy of the results produced by malicious cloud servers that perform outsourced decryption. In addition, it is not surprising that a large number of newly proposed CP-ABE systems, like the one in, use a combination of online/offline encryption and outsourced decryption techniques to maximise efficiency. In addition, sensitive data sharing applications, including healthcare data sharing and UAV data sharing, cannot employ typical CP-ABE systems because they cannot prevent privacy leaks in the access policy linked with shared ciphertexts. In order to address the issue, a partly hidden policy CPABE technique was suggested, which would provide policy security by the use of completely secure proofs. A privacy-preserving CP-ABE scheme with both expressive and hidden policies over a large attribute universe was devised by Zhang et al., while Lai et al. built an additional CP-ABE scheme with expressive and partial hidden access policies; both schemes achieve full security under the standard model. However, none of the aforementioned solutions address the root cause of user key misuse, which poses a threat of data loss due to unauthorized parties. A traceable and privacy-preserving CP-ABE technique with complete security was presented by Li et al. to address this difficulty. They drew inspiration from the white-box user tracking mechanism that was described in. Having a central CA and user list for tracing purposes is crucial to the system, however. A privacy-preserving and publicly traceable CP-ABE system was designed by Zeng et al. to reduce this dependency by combining the public user tracking approach from and. However, machines with low resources will not be able to take advantage of its great computing efficiency. Drones also provide massive amounts of usable, real-time

UAv data in this age of the Internet of Things. Massive data sets like these are very difficult to store. As UAV data is continually produced, the resources of a single cloud in cloud-based IoD may be exhausted due to a lack of scalability. To improve the scalability and flexibility of resources, distributed multi-cloud storage is essential. While Ren et al. established a blockchain-based multi-cloud storage method for smart homes, Li et al. brought DHT and blockchain techniques into distributed storage, contributing to this challenge. However, a complicated issue arises when it comes to distributed data access control in several kinds of cloud-based IoT systems. In a scenario with several clouds, Roy et al. suggested a strategy for controlling data access at granular levels, but they were unable to resolve the issue of dispersed data access. Thus, to address dispersed data access in various clouds, Li et al., Feng et al., and Liang et al. proposed several blockchain-based methods. The following distributed data access control systems are based on blockchain technology, which has led to its widespread use in secure and distributed data access control scenarios. But these plans hardly account for dispersed and multiple cloud storage. In light of the aforementioned difficulties, we build on our prior work PATLDAC to introduce BPADAC, a blockchain-based privacy-aware data access control scheme for cloud-based IoD data sharing that is both distributed and secure. BPADAC makes use of distributed ledger technology (DHT) for data storage and access, public and undeniable traceability, trustworthy access time limitation, and an attribute privacy protection technique.

2. DISCUSSION

For distributed and secure data exchange across UAVs in cloud-based IoD, the system suggests a privacy-aware data access control (BPADAC) method based on the blockchain. The improved scheme BPADAC builds on our earlier work PATLDAC, which provided fine-grained, traceable, and privacy-preserving UAV data access. It combines blockchain and Distributed Hash Table (DHT) techniques to further secure distributed UAV data storage and sharing in mobile cloud-based IoD. BPADAC's goals include distributed data access and storage, secure data sharing service provision, attribute privacy protection in access policies, undeniable and public traitor tracing, and reduced computation costs. In particular, the following are the improvements over our earlier work that this study introduces: • Data storage that can be scaled and is distributed. Traditional centralized cloud computing, which is used by most current systems and in our earlier work, is ineffective when it comes to handling large-scale and continuously growing UAV data. Therefore, BPADAC uses scalable, multi-cloud distributed data storage. Integrating blockchain and DHT algorithms

ensures its security and reliability, allowing linked numerous clouds to provide reliable and scalable resources for UAV data outsourcing. Similar to our earlier work PATLDAC, BPADAC protects access policies and user privacy by using a partly policy-hiding mechanism (for details, see Section V). Trustworthy data access that is distributed and has limits. With the use of blockchain technology for authentication and access control, data from unmanned aerial vehicles (UAVs) stored in numerous decentralized clouds may be accessed in a distributed fashion inside a distributed IoD system. By combining blockchain technology with access restriction techniques, BPADAC is able to accomplish what was missing in our earlier work—a trustworthy time limit for each valid user—when accessing data, which is essential for protecting UAV data sharing services from denial-of-service attacks that aim to exhaust cloud resources. • Public and indisputable traitor tracking; enhanced efficiency and safety. Without the requirement to maintain user lists in a centralized CA, any entity in the system may openly and efficiently identify traitors using BPADAC's public white-box tracing technique, which is designed to address key abuse problems. Nevertheless, BPADAC uses blockchain technology to record immutable proofs of treason for consistency tracking, so they can't refute the discovered malicious conduct evidence. In addition, BPADAC demonstrates superior performance in data encryption and decryption due to online/offline encryption and outsourced decryption testing methodologies, as shown by comprehensive efficiency analysis based on a large number of trials. Our prior work did not include the formal security model and evidence that we now provide for BPADAC.

3. MATERIALS AND METHODS

DC Activities including registering and logging in, requesting decryption key permission, seeing the status of that request, searching for data, and downloading it are all carried out by the DC in this module. DPwas In this section, he enters his credentials (username and password). Receiver actions, such as file uploads, willbeaccessibleafterlogin. BC The sector is able to do the following tasks in this module: Gain access to the cloud, see your files, and log in.TA The following tasks are available to the TA in this module: Step 1: Login. Step 2: View DC. Step 3: View DP.Step4:ViewDecKeyRequest.Step5:Authorize.ALOTOFCLOUD

Login, View All Permitted File Details, View Time Delay Results, and View Throughput Results are some of the functions that the Multi Cloud may do on a server that it maintains in order to provide data storage services.

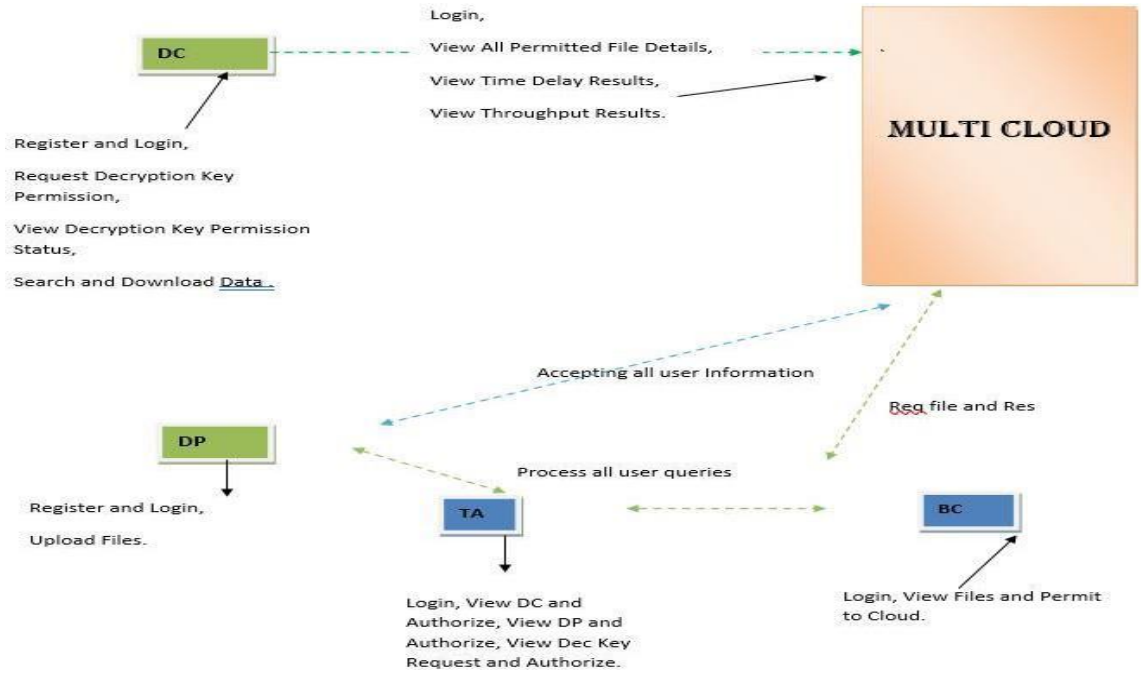

Figure 1: SYSTEM ARCHITECTURE IMPLEMENTATION

4. RESULTS

The system introduces a privacy-aware data access control (BPADAC) scheme that uses blockchain technology and distributed hash tables (DHTs) to ensure that data shared by unmanned aerial vehicles (UAVs) in a cloud-based IoD environment is both secure and accessible. The scheme also includes public and undeniable traceability, trustworthy access time limitations, and an attribute privacy protection method.

5. CONCLUSION

In this paper, we delve into the issues surrounding UAV data sharing in cloud-based IoT systems. Then, we present a scheme called BPADAC, which is based on blockchain technology. Its purpose is to facilitate secure and distributed UAV data sharing in a large-scale, mobile environment. We also provide the scheme's formal models, definitions, and

constructions. By combining blockchain technology with CP-ABE methodologies, BPADAC is able to provide distributed and fine-grained data access, allowing any authorized user to access UAV data over blockchain. Limited access periods are a means to ensure the UAV data sharing service in the meantime. The limitations of conventional centralized clouds may be eliminated by integrating multi-cloud with DHT technology, which allows for the distributed and scalable storage of large-scale UAV data. If you outsource your UAV data to the cloud, BPADAC will use partial policy concealing to keep your data private. Additionally, BPADAC can transparently and quickly handle traitor tracking by using a public user tracing technique, all without denying it. Also, BPADAC is safe and works well for UAV data sharing in cloud-based IoT systems, according to the results of the performance and security tests conducted on an Ethereum block chain prototype. We want to investigate the challenges associated with identifying UAV data sources and outsourcing UAV data in cloud-based IoD systems in our future research.

6. REFERENCES AND CITATIONS

[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,’’ *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16284–16296, Sep. 2022.

[5] S. Yu, A. K. Das, Y. Park, and P. Lorenz, ‘‘SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for Internet of Drones in smart city environments,’’ *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10374–10388, Oct. 2022.

[6] W. Wang, T. Chen, R. Ding, G. Seco-Granados, L. You, and X. Gao, ‘‘Location-based timing advance estimation for 5G integrated LEO satellite communications,’’ *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6002–6017, Jun. 2021.

[7] H. Xu, Z. Chen, H. Liu, L. Chang, T. Huang, S. Ye, L. Zhang, and C. Du, ‘‘Single-fed dual-circularly polarized stacked dielectric resonator antenna for K/Ka-bandUAVsatellite communications,’’ *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4449–4453, Apr. 2022.

[8] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, ‘‘A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks,’’ *Ad Hoc Netw.*, vol. 133, Aug. 2022, Art. no. 102894.

[9] Y. Dang, C. Benzaid, B. Yang, T. Taleb, and Y. Shen, ‘‘Deep ensemblelearning- based GPS spoofing detection for cellular-connected UAVs,’’ *IEEE Internet Things J.*, vol. 9, no. 24, pp. 25068–25085, Dec. 2022.

[10] J. Zhang, J. Ma, T. Li, and Q. Jiang, ‘‘Efficient hierarchical and timesensitive data sharing with user revocation in mobile crowdsensing,’’ *Secur. Commun. Netw.*, vol. 2021, pp. 1–17, Feb. 2021.

[11] W. Wang, T. Chen, R. Ding, G. Seco-Granados, L. You, and X. Gao, ‘‘Location-based timing advance estimation for 6G integrated LEO satellite communications,’’ *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 102–113, Jun. 2023.

[12] N. Tang, X. Chen, M. Zhao, and N. Kato, ‘‘The roadmap of communication and networking in 5G for the metaverse,’’ *IEEE Wireless Commun.*, early access, Jan. 09, 2023, doi: 10.1109/MWC.019.2100721.