A Privacy-Aware and Time-Limited Data Access Control Scheme with Large Universe and Public Traceability for Cloud-Based IoD

Jiawei Zhang[1], Yanbo Yang[2(✉)], Ning Lu[3], Zhiwei Liu[4], and Jianfeng Ma[1]

[1] School of Cyber Engineering, Xidian University, Xi'an, China
jfma@mail.xidian.edu.cn
[2] School of Information Engineering,
Inner Mongolia University of Science and Technology, Baotou, China
yangyanbo@imust.edu.cn
[3] College of Computer Science and Engineering, Northeastern University, Shenyang, China
luning@neuq.edu.cn
[4] The 27th Research Institute of China Electronics Technology Group Corporation, Beijing, China

Abstract. Recently, the rapid development of Internet of things (IoT) and 5G techniques has greatly facilitated the emerging applications of Unmanned Aerial Vehicles (UAVs) and the Internet of Drones (IoD). Moreover, Cloud-based IoD supplies an ideal platform for UAV data outsourcing and sharing services to lower their heavy burden. As UAV data are of high sensitivity, the convincing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can be employed to provide confidentiality and fine-grained access control for UAV data shared in cloud. However, the access policies related to encrypted UAV data usually consist of much sensitive and private information. Meanwhile, there exist misbehaving insiders of UAV data consumers that conduct unlimited access to disable UAV data sharing services, which is disastrous. Besides, the high computation overhead also extremely hinders resource-limited users in IoD. To seek a solution, we propose a privacy-aware and time-limited data access control (PATLDAC) scheme for secure UAV data sharing in Cloud-based IoD. Specifically, PATLDAC achieves user privacy preserving through partially hidden access policy which conceals the values of attributes while leaves their names with no sensitive information. Moreover, PATLDAC provide public user tracing to prevent user key abuse and limits the access time for each data user to guarantee service provision. In addition, PATLDAC realizes high efficiency in both encryption and decryption. Finally, the performance complexity evaluation indicate that PATLDAC is suitable and feasible for IoD systems.

Keywords: Internet of Drone · Cloud computing · CP-ABE · Hidden access policy · Limited access times

W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 103–116, 2022.
https://doi.org/10.1007/978-3-030-96791-8_8

1 Introduction

With the rapid development of Internet of Things (IoT) [15] and 5G communication [21] techniques, the application of Unmanned Aerial Vehicles (UAVs) encounters its vigorous advancement. Assisted by massive mobile access of 5G ground stations (GS) [12] and the strong connection ability among everything of IoT [2], UAVs can be deployed in various fields for task execution, and these interconnected UAVs facilitates the emerging Internet of Drone (IoD) [1] that enables service provision involving traffic supervision, disastrous rescue, good delivery and so on. In these attractive and practical applications supported by IoD, the kernel is the massive UAV data that are collected and utilized for analysis and predication [24]. Nevertheless, most of these applications need a huge volume of UAV data which exceed the computing and storage capability of resource-limited UAVs. To be a fortune, the cloud computing supplies an ideal platform to supply the massive UAV data with sufficient resources for outsourcing and processing and raises the CLoud-based IoD systems. However, due to most of the confidential tasks that UAVs are employed for, the huge amount of UAV data usually contains much sensitive and private information, including location-aware information, traffic related information, or even military-aware data. In the meantime, the outsourced UAV data in cloud makes its control out of the data producer, i.e., UAVs in IoV systems and vulnerable to various attacks. Therefore, how to guarantee the security of outsourced UAV data in cloud is a urgent requirement.

As a convincing solution for data security, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [28–30] enables the data producer to specify an access policy over a universe of attribute and enforce this access policy on encrypted outsourced data. Thus, it can be leveraged to guarantee the confidentiality and fine-grained access control for the massive UAV data outsourced in cloud. However, direct deployment of conventional CP-ABE schemes still faces several serous challenges to be addressed. The first challenge is the probable user privacy leakage in access policy. In conventional CP-ABE schemes, the access policy used to indicate the fine-grained access control for authorized data consumers is mostly in plaintext form. For example, an access policy "(SSN:1234 AND Role: Major General) OR (Department: Air Force AND State: Illinois)" will reflect that the consumer of the shared UAV data is a major general of air force office in Illinois state and that the UAV data may contains the information about Illinois. Thus, if these schemes are directly deployed in Cloud-based IoD systems for UAV data access control, any users that can approach the access policy can infer extra information of user privacy and sensitive information of UAV data, which will cause horrubke consequences, especially in military field. Although the schemes in [11,26,32] have been proposed to deal with the user privacy leakage in access policy by providing hidden access policy for CP-ABE schemes with fully security in standard model, they still lacks high efficiency in both encryption and decryption.

The second challenge is a long-lasting and intractable user key abuse problem in CP-ABE schemes, which is particularly significant when used in Cloud-based

IoD systems for UAV data access control. In most user key abuse attacks, authorized insiders prefer to leak their decryption keys to outsiders for extra profits gain. Especially, in military fields, the UAV data is of high value and cannot be shared with any other party. Thus, these miliary secret will bring huge profit if illegally shared with outsiders, which will give an inside traitor enough motivation to leak his decryption key. Nevertheless, in CP-ABE schemes, user decryption keys are related with their attribute set, which bring great difficulty to reveal the real identity of its owner. Hence, many traceable CP-ABE schemes are studied and designed to effectively disclose the traitors that leak their decryption keys by combining white-box mechanism with CP-ABE, that is, embedding the identity of data users to their decryption keys. Any time a leaked decryption key is captured, the identity of the owner will be discloused with white-box approach [13,14,19]. However, these schemes either suffer from high computation cost for user tracing or high storage overhead with a centralized user tracing authority. Therefore, to provide a public and efficient user traceable CP-ABE is a must for UAV data sharing in Cloud-based IoD systems.

The third challenge is the most common attack of Denial of Service in many service-oriented systems. As the Cloud-based IoD systems provides data sharing and outsourcing services to resource-limited UAVs and data consumers, if these services are disabled by attackers, the users will incur huge loss for it. Unfortunately, the prevention of this kind of attacks is out of consideration in most of CP-ABE schemes. For instance, an authorized but malicious user will launch DoS attack to the UAV dta sharing service by conducing continuous access which will cause great resource consumption of the services and eventually disable the service. Consequently, all other data consumers cannot access the UAV data sharing service, which is severe especially in military field and disastrous rescue applications. Thus, direct utilization of conventional CP-ABE scheme will make IoD systems vulnerable to DoS attacks by unlimited accessing to shared UAV data and disable the data sharing service to other valid users. Currently, there exist some related studies [7,25,34] that aims to limit the access time of data users for CP-ABE schemes, but they suffer from low efficiency in access verification, which are not suitable for time-sensitive applications of IoD. Thus, it is of great importance to provide efficient access time limitation method for CP-ABE schemes to adapt to UAV data sharing in Cloud-based IoD systems.

1.1 Current Research States

In UAV applications [10,18,22,27], data is a valuable resource that can be used for analysis and prediction [5,20]. Thus, the security of UAV data is most important. Ye et al. [24] designed a secure UAV system to protect the message transformed between UAVs. Then, Alladi [1] proposed an authentication scheme for UAV systems to guarantee the communication between UAVs and ground stations and Mehta et al. [16] integrated blockchain to 5G-enabled UAV to secure the UAV networks.

Ciphertext-Policy ABE (CP-ABE) [13,14,19,28–30] has been very popular in cloud data sharing for fine-grained access control. However, the traditional CP-

ABE schemes suffer from privacy leakage in access policy which is in plaintext and shared with ciphertext, which means they cannot be used in sensitive data sharing field. To address the problem, Zhang et al. [32] proposed a full secure partial hidden policy CP-ABE with large universe based on [9] with small attribute universe. However, these schemes fail to deal with user key abuse problem which may cause severe privacy and data disclosure. Thus, the scheme proposed in [11] introduced white-box user tracing mechanism into the scheme in [32] to realize user tracing, but it is a centralized tracing approach. Inspired by [31,33], the scheme in [26] proposed a partial hidden policy and public traceable CP-ABE, but it still incur high computation cost to be used in resource-limited devices.

Although CP-ABE is a promising and strong cyptographic tool, it also incurs heavy computation overhead in encryption and decryption which hinders its adoption. To solve these problem, the work in [6] introduces online/offline technique into ABE. Further, the authors in [23] integrates the idea to multi-authority CP-ABE schemes. Recently, many researches, i.e., [17] also combines online/offline into various ABE schemes. Meanwhile, to reduce the computation cost in decryption, the paradigm of outsourced decryption was introduced in [4]. Inspired by this, the scheme in [8] designed the verifiable outsourced decryption to resist malicious cloud and check if the messages are correctly decrypted. Recently, the literature [3] combines online/offline encryption and outsourced decryption for cost saving (Table 1).

Table 1. Function comparison in various schemes

Scheme	PH	LU	TLDAC	FS	SM	OOE	DT	VR	PT
Scheme [8]	✓	×	×	✓	✓	×	×	×	×
Scheme [17]	×	×	×	✓		✓	×	×	×
Scheme [6]	×	×	×	×	×	✓	×	×	×
Scheme [7]	×	✓	✓	×	×	×	×	×	×
Scheme [33]	×	✓	×	×	×	×	×	×	✓
Scheme [31]	×	✓	×	×	×	×	×	×	✓
Scheme [9]	✓	×	×	✓	✓	×	×	×	×
Scheme [32]	✓	✓	×	✓	✓	×	✓	×	×
Scheme [11]	✓	✓	×	×	×	✓	×	×	×
Scheme [26]	✓	✓	×	✓	✓	×	✓	×	✓
PATLDAC	✓	✓	✓	✓	✓	✓	✓	✓	✓

Note. PH: policy hiding; LU: large universe; TLDAC: time-limited data access; FS: full security; SM: standard model; OOE: online/offline encryption; DT: decryption test; VR: verifiability; PT: public traceability.

1.2 Motivation and Contributions

To address these challenges discussed above, in this paper, we propose a privacy-aware and time-limited data access control (PATLDAC) scheme for secure UAV data sharing in Cloud-based IoD to achieve both user privacy protection and limited access time along with efficient user tracing. To be specific, the main contributions are listed as follows:

- **Limited access time**. To counter the DoS attacks which conducts unlimited access to outsourced UAV data and guarantee the UAV data sharing service provision, PATLDAC can limits the access times for each valid user by impose a maximum access restriction to these users.
- **Partial hidden policy**. Our proposed PATLDAC achieves user privacy protection in access policy by separating each attribute in access policy into attribute name and attribute value while conceling the attribute values which may contain sensitive and private information.
- **Public user tracing**. To resist user key abuse problem, we introduce the public white-box tracing mechanism into our proposed PATLDAC scheme to guarantee that any traitor that intends to leak their decryption key for illegal profit will be efficiently revealed by anyone of the system in a public mode.

2 Preliminaries

2.1 Notations

In our work, $[l1, l2]$ is used to denote the set $\{l1, l1+1, \cdots, l2\}$ and $[n]$ is the set $1, 2, \cdots, n$, where $n \in Z_p^*$, while $|S|$ denotes the length of a string S.

2.2 Access Structure

Definition 1 *(Access Structures [28]). Let $E = E_1, \cdots, E_n$ be a entity collection. Given a set $C \subseteq 2^E \backslash \varnothing$, it is monotonic if $\forall D, F : D \subseteq F \bigcap D \in C \rightarrow F \in C$. Then, the set C is also a monotonic access structure and the subsets in C are called the authorized sets, otherwise, the unauthorized sets.*

2.3 Linear Secret Sharing Schemes (LSSS)

Definition 2 *(LSSS [30]). Let U be the attribute universe, where each attribute includes two parts: attribute name and its values. Each attribute has multiple values. An LSSS involves (A, ρ) on U, where A is an $l \times n$ matrix over Z_p which is called the share-generating matrix and ρ maps a row of A into an attribute name index. An LSSS consists of two algorithms.*

- *$Share((A, \rho), s)$: This algorithm is used to share a secret value s based on A. Considering a vector $\upsilon = (s, y_2, \ldots, y_n)^T$, where $s \in Z_p$ is the secret to be shared and $y_2, \cdots, y_n \in_R Z_p$, then $\lambda_x = A_x \cdot \upsilon$ is a share of the secret s corresponding to the attribute name indexed by $\rho(x)$.*

– *Reconstruction*$(\lambda_1, \cdots, \lambda_l, (A, \rho))$*: This algorithm is used to reconstruct s from secret shares. Let P be any authorized set and* $I = \{i|\rho(i) \in P\} \subseteq \{1, 2, \cdots, l\}$*, Then there exists coefficients* $\{w_i \in Z_p\}_{i \in I}$ *such that* $\sum_{i \in I} w_i A_i = (1, 0, \cdots, 0)$*. A subset I of* $\{1, 2, \cdots, l\}$ *is said to be a minimum authorized set of* (A, ρ) *if I satisfies* (A, ρ) *and any* $I^{'} \subset I$ *does not satisfy* (A, ρ)*. We define* $\mathbf{I}_{A,\rho}$ *as the set of subsets of* $\{1, 2, \cdots, l\}$ *that are minimum authorized sets of* (A, ρ)*.*

2.4 Composite Bilinear Map

Definition 3 *(Composite Bilinear Maps [29]):* *Composite order bilinear groups are widely used in IBE and ABE systems. We denote by G a group generator, which takes a security parameter* λ *as inputs and outputs a description of a bilinear group G. We define the output of G as* $(N, p_1, p_2, p_3, p_4, G, G_T, \hat{e})$ *with* $G = G_{p_1} \times G_{p_2} \times G_{p_3} \times G_{p_4}$*, where* p_1, p_2, p_3, p_4 *are distinct primes, G and* G_T *are cyclic groups of order* $N = p_1 p_2 p_3 p_4$*, and* $\hat{e} : G \times G \rightarrow G_T$ *is a bilinear map satisfy the following properties:*

– *Bilinear:* $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$*,* $\forall a, b \in Z_N, g, h \in G$*.*
– *Non-Degenerate: There exists* $g \in G$ *such that* $\hat{e}(g, g)$ *has order N in* G_T*.*
– *Computability: Assume group operations in G and* G_T *as well as the bilinear map* $\hat{e}$ *are computable in polynomial time with respect to the security parameter* λ

Let G_{p_i} *be the subgroup of big prime order* p_i*, where* $1 \leq i \leq 4$*. Note that for any* $X_i \in G_{p_i}, X_j \in G_{p_j}$*,* $\hat{e}(X_i, X_j) = 1$ *holds* $\forall i \neq j$*. The subgroups are said to be "orthogonal" to each other.*

3 The Proposed PATLDAC Scheme for UAV Data Sharing in Cloud-Based IoD

3.1 System Model

In this section, we give the description of the system model and design goals of our data access control scheme.

As shown in Fig. 1, our scheme involves four generic entities, Trusted Authority (TA), UAV Cloud Provider (UCP), Data Producer (DP) and Data Consumer (DC) which are described as follows.

(1) TA initializes the system and takes charge of the user registration and authorization. After receiving the attributes of users, TA generates secret key for users to empower their corresponding privileges.
(2) UCP is the UAV cloud provider that provides unlimited computation and storage resources together with data outsourcing services to UAVs. Moreover, UCP also supply data sharing services to authorized data consumers for their academic or industrial applications.

(3) DP is on behalf of UAVs that generate large number of spatiotemporal data that contain confidential information and have too large volume to be maintained in resource-limited UAVs. Thus, DP needs to encrypt these data for confidentiality and upload them to UCP for cost saving.
(4) DC is the consumer of UAV data for analysis and mining with machine learning related algorithms. Moreover, only authorized DCs have privileges to access the shared UAV data in UCP.

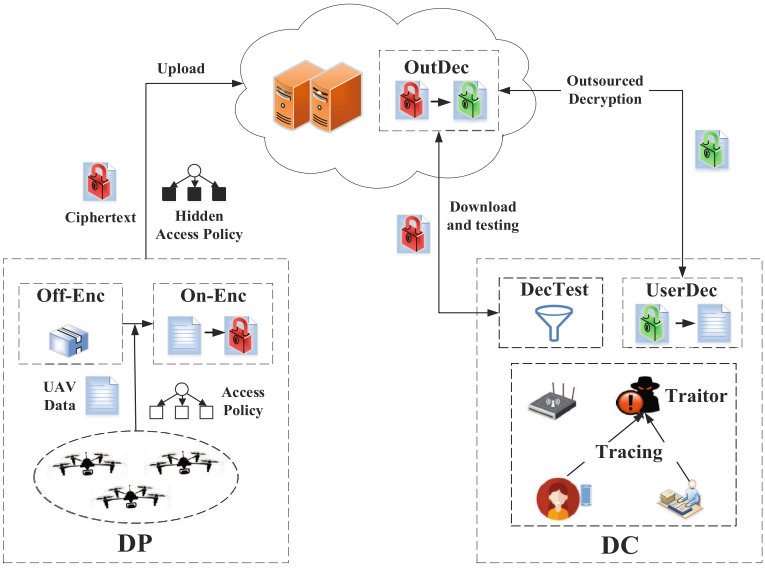

Fig. 1. The system model of our PATLDAC

We assume that the TA is a fully trusted entitiy while UCP is considered to be semi-honest which performs the pre-defined protocol honestly but is curious about the confidential information of UAV data. DP is regardes as trusted as it generates their own UAV data and uploads them to UCP for outsourcing. DC is considered to be malicious because part of them without enough privileges may intend to conduct unauthorized access and some of them may even perform unlimited access to disable the services. Moreover, there exists authorized but malicious insiders that prefer to leak their decryption keys for extra profits.

3.2 Design Goals

To confront these threats in system model, our proposal should satisfy following requirements:

- **Data confidentiality and fine-grained access control:** Due to the high level of confidentiality, the UAV data should be protected during communication among UAV, UCP and DCs, and their sharing in UCP. Moreover, only authorized DCs can obtain the content of the shared UAV data.
- **Privacy protection in access policy:** As the access policy may reveal the content of encrypted UAV data, it should be well protected in order to prevent sensitive information disclosure from being inferred by anyone accessible to shared UAV data.
- **Limited access times for authorized DCs:** To make sure the data sharing service can be available to valid DCs, it is preferable to limit the access time of each authorized DC such that no malicious insiders can conduct DoS/DDoS attacks to disable the services provided by UCP.
- **Public user tracing for malicious insiders:** The DCs that are authorized to access shared UAV data in UCP but attempt to acquire illegal benefit by leaking their decryption keys should be traced by anyone in system publicly.
- **Efficiency:** For the sake of resource-limited devices, it is preferable for DCs to save cost in encryption and efficiently test before data decryption to offset the high computational burden in decryption.

3.3 Concrete Construction

In our proposed PATLDAC, the basic building block is large universe and partial hidden policy CP-ABE. Based on this, PATLDAC integrates the feature of limited access time and public traceability to prevent malicious users who may conduct DoS attacks with unlimited data downloading and who intend to gain illegal profit by leaking their decryption keys. Thus, in the decryption process of PATLDAC, the UCP first checks if a DC have reached his upperlimit of access times. Besides, UCP also helps DCs to finish their decryption test and user decryption, which greatly save computation cost for decryption. Moreover, the user tracing mechanism is publicly executed by any entity of the system without a centralized authority.

- $Setup(\lambda) \rightarrow (PK, MSK)$: After TA receiving the security parameter λ, it invokes the bilinear group generator algorithm $\mathcal{G}(\lambda)$ to obtain a bilinear group $(N = p_1p_2p_3p_4, G, G_T, \hat{e})$, where $\{p_i\}_{i\in[4]}$ are different big primes and G, G_T are two cyclic groups of composite order N with a bilinear map $\hat{e} : G \times G \rightarrow G_T$ and a generator $g \in G$. Then, TA sets the attribute universe $U = Z_N$ and chooses $\alpha, a \in_R Z_N$, $f, h \in_R G_{(p_1)}$, $A_3 \in_R G_{p_3}$, $O, A_4 \in_R G_{p_4}$ and computes $B = \hat{e}(g, g)^\alpha, F = fO$. Besides, TA picks a collision resistant hash function $H_m : \{0, 1\}^* \rightarrow Z_N$. Finally, TA publishes the system public key as $PK = (N, g, g^a, h, B, F, A_4, H_m)$ and the master key is $MSK = (\alpha, f)$.
- $Setup_C(PK) \rightarrow (ctr, L, ST)$: Given the system public key PK, the UCP generates an initial counter $ctr = 0$ for data sharing service and an empty state set ST for each DC in user universe. The UCP also initiates a list L to maintain the ctr and ST for each DC.

- $Setup_U(PK) \rightarrow (pk_u, sk_u)$: On inputting the system public key PK, each DC chooses a random number $z_u \in_R Z_N$ as secret key $SK_u = z_u$ and publishes the user public key as $PK_u = h^{z_u}$.
- $KeyGen(PK, MK, PK_u, ID_u, S) \rightarrow DK_u$: After receiving the system public key PK, the decryption key request from DC with his identity ID_u and attribute set $\mathcal{S} = (I_s, S)$, where $I_s \subset Z_N$ is the index of each attribute in S and $S = \{s_i\}_{i \in I_s}$ is the attribute value of the DC, TA randomly chooses $t \in Z_N$ and $R, R^{'}, R_i \in G_{p_3}$ for $i \in I_s$. TA finally outputs the decryption key of DC $DK_u = \{\mathcal{S}, K, K^{'}, K^{''}, \{K_i\}_{i \in I_s}\}$, where

$$K = g^{\alpha} g^{atH_m(K^{'}, K^{''})} R, K^{'} = g^t R^{'}, K^{''} = ID_u, K_i = (g^{s_i} f)^t R_i$$

- $KeyGen_{OUT}(PK, DK_u, SK_u, csi) \rightarrow TK_u$: DC takes the system public key PK, his decryption key DK_u and secret key SK_u with current state information csi as input, then he computes $TK_u^1 = \{I_s, K^1 = g^{z_u} \cdot K = g^{z_u} g^{\alpha} g^{atH_m(K^{'}, K^{'})}, K^{'}, K^{''}, \{K_i\}_{i \in I_s}\}$. Then, the DC calculates the rest components $K_c = B^{1/(z_u + H_m(csi))}$, $K_p = g^{1/(z_u + H_m(csi))}$. Finally, the DC gets his transformation key $TK_u = (TK_u^1, K_c, K_p, csi)$.
- $Encrypt_{off}(PK) \rightarrow IT_t$: Given the system public key PK, each DP prepares the encryption process in advance. DP selects random values $s, s^{'} \in Z_N$ as secret value for sharing to compute $\widetilde{C}_{\delta}^{'} = B^{s^{'}}, \widetilde{C}_1^{'} = B^s, \widehat{C}_{\delta}^{'} = g^{s^{'}}, \widehat{C}_1^{'} = g^s$ and constructs a intermediary pool $IT_1 = \{(s, s^{'}, \widetilde{C}_{\delta}^{'}, \widetilde{C}_1^{'}, \widehat{C}_{\delta}^{'}, \widehat{C}_1^{'})\}$. Then, DP chooses $\lambda^{'}, t^{'}, r^{'} \in_R Z_N$ and calculates $C_{\delta,x}^{'} = g^{a\lambda^{'}}, C_{1,x}^{'} = g^{a\lambda^{'}} (g^{t^{'}} F)^{r^{'}}, C_{2,x}^{'} = g^{r^{'}}$ to construct another intermediary pool $IT_2 = \{(\lambda^{'}, t^{'}, r^{'}, C_{\delta,x}^{'}, C_{1,x}^{'}, C_{2,x}^{'})\}$. Finally, DP outputs an intermediate ciphertext $IT_t = \{IT_1, IT_2\}$.
- $Encrypt_{on}(PK, IT_t, M, \mathcal{A}) \rightarrow CT$: On inputting the system public key PK, the intermediate cihertext IT_t, the UAV data M with designated access policy $\mathcal{A} = \{A, \rho, \mathcal{T}\}$, where A is a $l \times n$ share-generating matrix and $\mathcal{T} = \{t_{\rho(1)}, \cdots, t_{\rho(l)}\}$ is the value set of the access policy $\mathcal{A}$, DP chooses a random tuple $(s, s^{'}, \widetilde{C}_{\delta}^{'}, \widetilde{C}_1^{'}, \widehat{C}_{\delta}^{'}, \widehat{C}_1^{'})$ from IT_1 and two random vectors $v = (s, v_2, \cdots, v_n), v^{'} = (s^{'}, v_2^{'}, \cdots, v_n^{'})$ of n dimentions over Z_N, where $s, s^{'} \in_R Z_N^n$ are the shared secret value. DP also picks l different random tuples $\{(\lambda_x^{'}, t_x^{'}, r_x^{'}, C_{\delta,x}^{'}, C_{1,x}^{'}, C_{2,x}^{'})\}_{x \in [l]}$ from IT_2. Besides, DP chooses $O_{\delta} \in_R G_{p_4}$ and $O_{\delta,x}, O_{c,x}, O_{d,x} \in_R G_{p_4}$, where $1 \leq x \leq l$. Then, DP can calculate the ciphertext $CT = \{(A, \rho), \widetilde{C_{\delta}}, \widehat{C_{\delta}}, \{C_{\delta,x}\}_{1 \leq x \leq l}, \widetilde{C_1}, \widehat{C_1}, \{C_{1,x}, C_{2,x}, C_{3,x}, C_{4,x}, C_{5,x}\}_{1 \leq x \leq l}\}$, where

$$\widetilde{C_{\delta}} = \widetilde{C_{\delta}}^{'}, \widehat{C_{\delta}} = \widehat{C_{\delta}}^{'} \cdot O_{\delta}, C_{\delta,x} = C_{\delta,x}^{'} \cdot (g^{t_{\rho(x)}} F)^{-s^{'}} O_{c,x},$$

$$\widetilde{C_1} = M \cdot \widetilde{C_1}^{'}, \widehat{C_1} = \widehat{C_1}^{'}, C_{1,x} = C_{1,x}^{'} \cdot O_{c,x}, C_{2,x} = C_{2,x}^{'} \cdot O_{d,x},$$

$$C_{3,x} = A_x \cdot v - \lambda_x^{'}, C_{4,x} = A_x \cdot v^{'} - \lambda_x^{'}, C_{5,x} = r_x^{'}(t_{\rho(x)} - t_x^{'})$$

Finally, DP uploads the ciphertext CT to UCP for data outsourcing and sharing.

– $DecryptTest(PK, CT, TK_u, SK_u) \rightarrow True/False$: The algorithm is an interaction between UCP and DC as below.
  - After receiving the system public key PK and the UAV data access request from DC with his transformation key TK_u, UCP first checks if the access time of the DC reach the maximum as follows:
    1) $\hat{e}(g^{H_m(csi)} \cdot Z_u, K_p) = E$ and $K_c = \hat{e}(g \cdot Z_u, K_p)$;
    2) $ctr + 1 \leq \varepsilon$, where ε is the maximum access time of the outsourced decryption service request for UAV data sharing;
    3) $K_c \notin ST$.

    If the above equations do not hold, UCP prohibit the further data access for the DC. Otherwise, UCP updates $ctr = ctr + 1$ and stores K_c in ST for future use.
  - UCP calculates $I_{A,\rho} \subset \{1, 2, \cdots, l\}$ that satisfies the partial hidden access policy (A, ρ) of CT and the following equation:

$$P_0 = \hat{e}(\prod_{i \in I} C_{\delta,i}^{w_i}, (K^{'})^{H_m(K^{'}, K^{''})}) \cdot \hat{e}(\widehat{C_\delta}, K^{-1} \prod_{i \in I} K_{\rho(i)}^{w_i}),$$

$$P_1 = \frac{\hat{e}(\widehat{C_1}, K)}{\prod_{i \in I}(\hat{e}(C_{1,i}, K^{'})\hat{e}(C_{2,i}, K_{\rho(i)}))^{w_i}} = \hat{e}(g, g)^{\alpha s}\hat{e}(g, g)^{z_u s}$$

    Then, UCP allows the DC to download the ciphertext CT and returns P_0, P_1 to DC.

– $UserDec(PK, CT, P_0, P_1, SK_u)$: With the system public key PK and secret key SK_u, DC computes following to check if there exists a subset $I \in I_{A,\rho}$ that satisfies $\{\rho(i) | i \in I\} \subseteq I_s$ and checks the following equation

$$\widetilde{C_\delta}^{-1} \stackrel{?}{=} P_0 \cdot \hat{e}(g^{SK_u}, \widehat{C_\delta})$$

where $\sum_{i \in I} w_i A_i = (1, 0, \cdots, 0)$ for some constants $w_{i i \in I}$. If no such I exists, it outputs $\perp$ to indicate that attribute set S of the DC does not satisfy the partially hidden access policy (A, ρ). Otherwise, the ciphertext is valid and authorized and the DC can calculate the following equation:

$$M = \widetilde{C_1} \cdot \hat{e}(g^{SK_u}, \widehat{C_1})/P_1$$

Finally, DC gets the plaintext M of the shared UAV data.

– $UTrace(PK, DK_u) \rightarrow ID$ or $null$: Given the system public key PK and the leaked decryption key DK_u, anyone of the system can execute the algorithm. First, it checks if $DK_u = \{\mathcal{S}, K, K^{'}, K^{''}, \{K_i\}_{i \in I_s}\}$ and its components satisfies $K, K^{'}, K_i \in G, K^{''} \in Z_N$. Then, the algorithm executes

Key Sanity Check:

$$\hat{e}(g, K) = B \cdot \hat{e}(g^a, (K^{'})^{H_m(K^{'}, K^{''})}) \tag{1}$$

If the decryption key DK_u does not satisfy **Key Sanity Check**, the algorithm abort and outputs $null$. Otherwise, we consider it as a well-formed decryption key. Then, the algorithm outputs the real identity of the owner as $ID_u = K^{''}$.

4 Analysis of Our PATLDAC Scheme

This section demonstrates the theoretical analysis of our proposed PATLDAC scheme in Table 2 and Table 3.

We analyze the complexity of our scheme and three related schemes in [11, 26, 32]. Here, we let E and E_T denote exponentiation in group G and G_T, P denote pairing operation in $\hat{e}$, $|S|$ denotes the number of access attribute set S, $|G_{p_i}|$, $|G_{p_i p_j}|$, $|G_T|$ and $|Z_N|$ denote the length of element of G_{p_i}, $G_{p_i} \cdot G_{p_j}$, G_T and Z_N.

Table 2. Computation comparison in various schemes

Schemes	KeyGen	UserEnc
[32]	$(2\|S\|+3)E$	$(7l+4)E+2E_T$
[11]	$(2\|S\|+4)E$	$(7l+5)E+2E_T$
[26]	$(2\|S\|+3)E$	$(6l+2)E+2E_T$
PATLDAC	$(2\|S\|+3)E$	$2\|S\|E$
Schemes	UserDec	UserTrace
[32]	$2\|I\|E+(\|I\|+1)E_T+(2\|I\|+3)P$	–
[11]	$(3\|I\|+4)E+(\|I\|+1)E_T+(2\|I\|+4)P$	$(2\|S\|+2)E+(2\|S\|+5)P$
[26]	$(4\|I\|+4)E+E_T+4P$	$E+2P$
PATLDAC	$2E$	$E+2P$

Note. "l" is the row number in access policy, "$|I|$" is the complexity of access policy in decryption.

From the view of computation complexity, we emphases on the aspects of the time cost in $KeyGen, UserEnc, UserDec, UserTrace$. To demonstrate the advantage of our proposal, we compare the computation complexity between PATLDAC and [11, 26, 32] summarized in Table 2. Specifically, the time cost in $KeyGen$ algorithm in PATLDAC is just the same as that of [26, 32] while less than that of [11] which needs centralized traceability. Moreover, the time cost in $UserEnc$ of PATLDAC is much less than that of other three schemes as it utilizes online/offline encryption to offload the complex attribute-related computations to offline phase. More important, the time cost in $UserDec$ algorithm is only $2E$ which is also significantly less than others. In addition, the time cost in $UserTrace$ of PATLDAC is the same as that of [26] and much less than that of [11] which incurs extra cost for attribute-related operations in key sanity check.

From the view of storage complexity, we emphases on the aspects of the storage cost in $Setup, KeyGen, UserEnc, UserTrace$. To demonstrate the advantage of our proposal, we compare the storage complexity between PATLDAC and [11, 26, 32] summarized in Table 3. It is obvious that the size of system public key of PATLDAC is the same as that of [11] while more than the other two as it introduces another one element in G for user public key generation to realize outsourced decryption in standard model. In the storage cost of user decryption

Table 3. Storage comparison in various schemes

Schemesl	PPSize	DKSize	CTSize	TraceSize
[32]	$4\|G_{p_i}\| + \|G_T\|$	$(\|S\|+2)\|G_{p_ip_j}\|$	$(2l+3)\|G_{p_ip_j}\| + 2\|G_T\|$	–
[11]	$5\|G_{p_i}\| + \|G_T\|$	$(\|S\|+3)\|G_{p_ip_j}\| + \|Z_N\|$	$(3l+4)\|G_{p_ip_j}\| + 2\|G_T\|$	$\|L\|\|Z_N\|$
[26]	$4\|G_{p_i}\| + \|G_T\|$	$(\|S\|+2)\|G_{p_ip_j}\| + \|Z_N\|$	$(2l+2)\|G_{p_ip_j}\| + 2\|G_T\|$	$\odot$
PATLDAC	$5\|G_{p_i}\| + \|G_T\|$	$(\|S\|+2)\|G_{p_ip_j}\| + \|Z_N\|$	$(2l+3)\|G_{p_ip_j}\| + 2\|G_T\| + 3l\|Z_N\|$	$\odot$

Note. "$|L|$" is the size of user table for tracing, "$\odot$" is the efficient symbol.

key, PATLDAC is the same as [26] and less than that of [11] for centralized user tracing. The ciphertext size in PATLDAC is somewhat more than the other schemes as it introduces extra three elements in Z_N for online/offline encryption to achieve cost saving. Most important, PATLDAC and the scheme in [26] realize high efficiency in user tracing, which is much less than that of [11].

5 Conclusion

In this paper, we proposed a privacy-aware and time-limited data access control (PATLDAC) scheme for secure UAV data sharing in Cloud-based IoD system. The proposed PATLDAC can achieve user privacy preserving in access policy through partially hidden access policy to conceal the values of attributes while leaves their names with no sensitive information. To resist user key abuse efficiently, PATLDAC provided public user tracing. In the meantime, for the security of data sharing security to guarantee service provision, PATLDAC supports data access time limitation that each data consumer can only perform a maximum times of access to shared UAV data. In addition, PATLDAC realize high efficiency in both encryption and decryption. The complexity analysis and comparison show that PATLDAC is suitable for IoD systems.

Acknowledgment. This work is supported by Natural Science Foundation of Inner Mongolia, China, 2020 (No. 2020LH06007), Innovation Fund of Inner Mongolia University of Science and Technology, China (No. 2019QDL-B51) and Inner Mongolia Major science and technology projects: artificial intelligence application technology and product research, development Application Research and demonstration in modern pastures (2019ZD025).

References

1. Alladi, T., Bansal, G., Chamola, V., Guizani, M., et al.: SecAuthUAV: a novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans. Veh. Technol. **69**(12), 15068–15077 (2020)
2. Boursianis, A.D., et al.: Internet of Things (IoT) and agricultural unmanned aerial vehicles (UAVs) in smart farming: a comprehensive review. Internet of Things, p. 100187 (2020)
3. De, S.J., Ruj, S.: Efficient decentralized attribute based access control for mobile clouds. IEEE Trans. Cloud Comput. **8**(01), 124–137 (2020)

4. Green, M., Hohenberger, S., Waters, B., et al.: Outsourcing the decryption of ABE ciphertexts. In: USENIX Security Symposium, vol. 2011 (2011)
5. Gupta, L., Jain, R., Vaszkun, G.: Survey of important issues in UAV communication networks. IEEE Commun. Surv. Tutor. **18**(2), 1123–1152 (2015)
6. Hohenberger, S., Waters, B.: Online/offline attribute-based encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 293–310. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_17
7. Hong, J., Xue, K., Gai, N., Wei, D.S., Hong, P.: Service outsourcing in F2C architecture with attribute-based anonymous access control and bounded service number. IEEE Trans. Dependable Secure Comput. **17**(5), 1051–1062 (2018)
8. Lai, J., Deng, R.H., Guan, C., Weng, J.: Attribute-based encryption with verifiable outsourced decryption. IEEE Trans. Inf. Forensics Secur. **8**(8), 1343–1354 (2013)
9. Lai, J., Deng, R.H., Li, Y.: Expressive CP-ABE with partially hidden access structures. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp. 18–19 (2012)
10. Li, M., Cheng, N., Gao, J., Wang, Y., Zhao, L., Shen, X.: Energy-efficient UAV-assisted mobile edge computing: resource allocation and trajectory optimization. IEEE Trans. Veh. Technol. **69**(3), 3424–3438 (2020)
11. Li, Q., Zhang, Y., Zhang, T., Huang, H., Xiong, J.: HTAC: fine-grained policy-hiding and traceable access control in mhealth. IEEE Access **PP**(99), 1 (2020)
12. Li, X., Zhou, R., Zhang, Y.J.A., Jiao, L., Li, Z.: Smart vehicular communication via 5G mmWaves. Comput. Netw. **172**, 107173 (2020)
13. Liu, Z., Duan, S., Zhou, P., Wang, B.: Traceable-then-revocable ciphertext-policy attribute-based encryption scheme. Futur. Gener. Comput. Syst. **93**, 903–913 (2019)
14. Liu, Z., Xu, J., Liu, Y., Wang, B.: Updatable ciphertext-policy attribute-based encryption scheme with traceability and revocability. IEEE Access **7**, 66832–66844 (2019)
15. Lv, Z., Qiao, L., Li, J., Song, H.: Deep-learning-enabled security issues in the internet of things. IEEE Internet Things J. **8**(12), 9531–9538 (2020)
16. Mehta, P., Gupta, R., Tanwar, S.: Blockchain envisioned UAV networks: challenges, solutions, and comparisons. Comput. Commun. **151**, 518–538 (2020)
17. Miao, Y., Tong, Q., Choo, K.K.R., Liu, X., Deng, R.H., Li, H.: Secure online/offline data sharing framework for cloud-assisted industrial internet of things. IEEE Internet Things J. **6**(5), 8681–8691 (2019)
18. Mukherjee, A., Misra, S., Chandra, V.S.P., Obaidat, M.S.: Resource-optimized multiarmed bandit-based offload path selection in edge UAV swarms. IEEE Internet Things J. **6**(3), 4889–4896 (2018)
19. Ning, J., Dong, X., Cao, Z., Wei, L.: Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In: Pernul, G., Ryan, P.Y.A., Weippl, E. (eds.) ESORICS 2015. LNCS, vol. 9327, pp. 270–289. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24177-7_14
20. Pathak, N., Misra, S., Mukherjee, A., Roy, A., Zomaya, A.Y.: UAV virtualization for enabling heterogeneous and persistent UAV-as-a-service. IEEE Trans. Veh. Technol. **69**(6), 6731–6738 (2020)
21. Wazid, M., Das, A.K., Shetty, S., Gope, P., Rodrigues, J.J.: Security in 5G-enabled internet of things communication: issues, challenges, and future research roadmap. IEEE Access **9**, 4466–4489 (2020)

22. Wu, Q., Zeng, Y., Zhang, R.: Joint trajectory and communication design for multi-UAV enabled wireless networks. IEEE Trans. Wirel. Commun. **17**(3), 2109–2121 (2018)
23. Xue, K., et al.: RAAC: robust and auditable access control with multiple attribute authorities for public cloud storage. IEEE Trans. Inf. Forensics Secur. **12**(4), 953–967 (2017)
24. Ye, J., Zhang, C., Lei, H., Pan, G., Ding, Z.: Secure UAV-to-UAV systems with spatially random UAVs. IEEE Wirel. Commun. Lett. **8**(2), 564–567 (2018)
25. Yuen, T.H., Liu, J.K., Au, M.H., Huang, X., Susilo, W., Zhou, J.: *k*-times attribute-based anonymous access control for cloud computing. IEEE Trans. Comput. **9**(64), 2595–2608 (2015)
26. Zeng, P., Zhang, Z., Lu, R., Choo, K.K.R.: Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things. IEEE Internet of Things J. (2021)
27. Zeng, Y., Zhang, R.: Energy-efficient UAV communication with trajectory optimization. IEEE Trans. Wirel. Commun. **16**(6), 3747–3760 (2017)
28. Zhang, J., Li, T., Obaidat, M.S., Lin, C., Ma, J.: Enabling efficient data sharing with auditable user revocation for IoV systems. IEEE Syst. J. (2021)
29. Zhang, J., Ma, J., Li, T., Jiang, Q.: Efficient hierarchical and time-sensitive data sharing with user revocation in mobile crowdsensing. Secur. Commun. Netw. **2021** (2021)
30. Zhang, J., et al.: Efficient hierarchical data access control for resource-limited users in cloud-based e-health. In: 2019 International Conference on Networking and Network Applications (NaNA), pp. 319–324. IEEE (2019)
31. Zhang, K., Li, H., Ma, J., Liu, X.: Efficient large-universe multi-authority ciphertext-policy attribute-based encryption with white-box traceability. Sci. China Inf. Sci. **61**(3), 1–13 (2017). https://doi.org/10.1007/s11432-016-9019-8
32. Zhang, Y., Zheng, D., Deng, R.H.: Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J. **5**(3), 2130–2145 (2018)
33. Zhang, Z., Zeng, P., Pan, B., Choo, K.K.R.: Large-universe attribute-based encryption with public traceability for cloud storage. IEEE Internet Things J. **7**(10), 10314–10323 (2020)
34. Zhou, J., Cao, Z., Qin, Z., Dong, X., Ren, K.: LPPA: lightweight privacy-preserving authentication from efficient multi-key secure outsourced computation for location-based services in VANETs. IEEE Trans. Inf. Forensics Secur. **15**, 420–434 (2019)