# Auditable and Times limitable Secure Data Access Control for Cloud-based Industrial Internet of Things

Teng Li[1], Jiawei Zhang[1], Yanbo Yang[2], Wei Qiao[1],and Yangxu Lin[1]
[1]School of Cyber Engineering, Xidian University, Shaanxi, China
[2]School of Information Engineering, Inner Mongolia University of Science & Technology, China

**Recently, the rapid development of Internet of things (IoT) and cloud computing technologies have greatly facilitated various industrial applications and Industrial IoT (IIoT). The widely deployed IIoT devices and large capacity of cloud significantly benefit for and bring convenience to various industrial sectors. However, there exist a large number of concerns about data security in IIoT, especially when a majority of sensitive IIoT data is shared in cloud. Although as one of the most promising technique, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) can provide fine-grained access control for IIoT data shared in cloud, there are still many drawbacks which impede the direct adoption of conventional CP-ABE. On the one hand, unlimited IIoT data access times may disable data access service of cloud and bring serious consequences. On the other hand, the access policies of ciphertexts usually consist of much sensitive information and cause privacy exposure. Moreover, the high computation overhead also extremely hinders resource-limited users in IIoT applications. To solve these problems, we propose TAHP-CP-ABE, a k-times and auditable hidden-policy CP-ABE scheme which is suitable for resource-limited users and privacy-aware access policies with data access times limitation in IIoT applications. Specifically, TAHP-CP-ABE preserves the privacy of access policies by hiding only attribute values and realizes limited access times as well as efficient IIoT ciphertexts decryption with decryption test and outsourced decryption. The security analysis and experimental results indicate that TAHP-CP-ABE is secure, efficient and practical.**

***Index Terms*—CP-ABE, privacy-preserving, cloud-assisted IIoT, access times limitation, auditable outsourced decryption.**

## I. Introduction

RECENTLY, the technologies of Internet of things (IoT) [1] and cloud computing [2] have greatly promoted the advent of Industrial IoT (IIoT). The explosive increase of the IIoT devices in various industrial sectors, such as healthcare, manufacturing, etc, have greately benefited their development. Further, the cloud-assisted IIoT [3], as a promising paradigm, enables the gathering, storage, managing and sharing for important IIoT data with sophisticated analysis and monitoring [4]. All data collected from IIoT devices will be outsourced to cloud in order to lower the burden for the pervasive IIoT devices which has limited computation and storage resources. The outsourced data can be shared by industrial users for business usage or remote monitoring. However, the sensitive information contained in the shared IIoT data brings many security issues, which may be leaked and violated if maliciously accessed by unauthorized parties. Thus, access control is of great importance for data security in cloud-assisted IIoT environment.

To protect data security for cloud-assisted IIoT, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [5], [6], as a promising technique, can be utilized to enforce fine-grained access control over shared IIoT data. It enables the data owner to specify an access policy over a universe of attribute and enforce corresponding access control in data access process. However, when applied in IIoT applications, the traditional CP-ABE must be adapted to address the above scenarios. The access policies of traditional CP-ABE are in cleartext form and outsourced to cloud together with ciphertext, which may contain much private information. Thus, there is no difficulty for an unauthorized user to get the sensitive information in access policies [7]. For instance, a manufacturing factory can encrypt its IIoT data under access policy "(SSN:1234 AND gender: male) OR (Department: tyre manufacturing AND Organization: Center Factory)". The policy means that the shared IIoT data can be accessed by a industrial user from center factory whose position is tyre manufacturing or a male user with identity, such as social security number (SSN) "1234". Anyone including Cloud Service Provider (CSP) can infer from the access policy that a male user with SSN "1234" is working on tyre manufacturing in central factory. This leaks users' privacy and demonstrates the necessity of hiding access policies in traditional CP-ABE.

More importantly, the data sharing service availability is significant for data users in IIoT applications, especially those sectors manufacturing key machines [8]. As the data sharing service of cloud-assisted IIoT applications is usually provided through Internet, it suffers from various attacks from potential malicious users by unlimited access the data sharing service in a short time period which can easily disable the cloud service and prevent all users from accessing the shared data [9]. For example, a Unmanned Aerial Vehicle (UAV) manufacturer selects public cloud to outsource their data about UAV manufacturing authomatically. All supervisors can sharing the important manufacturing data from public cloud through Internet. If a malicious user, no matter insider or outsider, launches unlimited data access, the data sharing service will easily be unavailable for users. This may disable the important data sharing service and what is more, it can prevent supervisors from obtain the latest UAV manufacturing data, which leads to unthinkable consequences. As a result, to restrict the data access time is also very important for data sharing services in cloud-assisted IIoT and makes sense for

Manuscript received November 9, 2021; revised January 17, 2022. Corresponding author: Teng Li (email: litengxidian@gmail.com).

IIoT applications.

In the meantime, to improve the efficiency of decryption for tranditional CP-ABE schemes, many studies introduces outsourced decryption [10]–[12] to move a majority of decryption compuation task to cloud and leave only constant and very little computation in user decryption. However, if the cloud is corrupted or becomes lazy due to cost saving, it may returns back the false results to users when supplying outsourced decryption service. Thus, it is necessary to check if the result from cloud in outsourced decryption, which facilitate many verifiable outsourced CP-ABE schemes in previous studies [13], [14]. Nevertheless, these schemes incur extra compuation and storage cost for result verification in outsourced decryption, which obviously adds heavier burden on users' resource-limited devices [15]. Thus, to find a lightweight verification approach for outsourced decryption is a big challenge for current CP-ABE schemes.

In this paper, we propose a k-Times and Auditable Hidden-Policy CP-ABE (TAHP-CP-ABE) to address these issues discussed above. TAHP-CP-ABE can partially hide the access policies, that is, the sensitive attribute values will be hidden in encrypted IIoT data while left the attribute names in clear text which will be sent with encrypted IIoT data. In order to realize more fine-grained access control and improve efficiency, we enforce access times limitation on shared data and introduce decryption test and decryption outsourcing technique to lower the computation burden of resource-limited devices and improve the efficiency. To be specific, our main contributions are listed as follows:

- **Limited access time**. TAHP-CP-ABE provides the property of data access times limitation for each valid user to prevent them from unlimited accessing shared IIoT data in cloud which may disable data sharing service.
- **Partial hidden policy**. TAHP-CP-ABE achieves user privacy protection in access policy by seperating each attribute in access policy into attribute name and attribute value while conceling the attribute values which may contain sensitive and private information.
- **Data auditing and high efficiency**. To guarantee the correctness of outsourced decryption of cloud, TAHP-CP-ABE support data auditing for the transformed ciphertext from cloud to verify its correctness. Moreover, TAHP-CP-ABE greately improves the efficiency in encryption and decryption by online/offline technique and outsourced computing techniques.

The rest of this paper is organized as follows. In Section II, we review some existing studies related to our proposal. In Section III, we introduce the preliminaries including some definitions and notations used in our proposal. In Section IV, we give the system model, threat model, design goal as well as security model. The overview and the construction of our proposal is presented in Section V. Following this, in section VI, we discuss the security analysis and the performance evaluation of our work. Finally, the conclusion of our work will be given in Section VII.

## II. Related Work

As a promising tool of fine-grained access control, Ciphertext-Policy ABE (CP-ABE) [6] was designed on the basis of [5], which is usually utilized with user authentication approaches [16]–[21] for data access control. For CP-ABE, it can enforce flexible access policy on encrypted data for data owners and has been well accepted for data access control on behalf of data owner. Thus, it has been studied by many researches in [8], [22]–[25] since its proposal in [26].

For the efficiency improvement in encryption, the study in the literature [27] first devised the online/offline technique into encrytion schemes, e.g, identity-based encryption on the basis of online/offline digital signatures proposed in [28] and online/offline Chameleon hashing functions [29] suitable for resource-constrained devices, such as IIoT devices. Later, the study in [30] proposed first online/offline ABE scheme based on the idea of online/offline technique that includes online and offline phase in which the former phase incurs very little cost on user devices as all major computations are moved to the latter phase while the resource-constrained devices are being charged. Based on this, some fully secure online/offline schemes were proposed in [31], [32]. To make sure online/offline encryption is correctly executed, the scheme in [33] proposed a verifiable outsourced encryption scheme as well as a batch verification for outsourced encrypiton.

As the high cost in decrypiton computation of traditional CP-ABE schemes impedes its widely adoption, the literature [10] designed a lightweight ABE scheme to reduce the decrypiton computation to a constant number of pairing operations but it adds the storage of keys. As a solution, the schemes in [11], [12], [34] introduced outsourced decryption CP-ABE by outsourcing the expensive operations in decryption to a third party and leave just a constant number of operations in user devices. Whereas, the security of these schemes rely on a trusted or semi-trusted third party. To ensure the data security of outsourced decryption, the literature [13] devised the notion of verifiable outsourced decryption ABE and motivated the work in [14] that proposes an efficient verifiable outsourced decryption ABE scheme which supports the verification for the correctness of the transformed ciphertext. Subsequently, many relevant schemes are proposed for verifiable outsourced decryption in ABE, such as [15]. To further improve the security and convenience of data security in verifiability, many schemes [35]–[38] are proposed which utilize the immutability of blockchain to achieve efficient and secure data verifiability and auditability.

Although a numerous number of studies on CP-ABE scheme, access policy privacy preserving is still a serous problem with probable privacy leakage. To address the issue, the study in [39] presented partial hidden-policy CP-ABE by concealling the value of attributes in access policy but it supports only "AND" gate policy. Subsequently, Lai et al. [40] introduced expressiveness into its partial policy-hidden CP-ABE scheme [41] and spreaded the work in [7], [42]–[44] that support both decryption testing and large attribute universe, but the these schemes are implemented over composite order groups. Thus, Cui et al. [45], [46] designed two partial policy hidden CP-ABE schemes based on prime order groups that supports expressive access policy and verifiability. Moreover, these CP-ABE schemes are weak in security as their exposed attribute names in access policy. As a solution, Zhou et al. [47] introduced broadcast encryption into CP-ABE to achieve fully hidden policy, but it incurs extra computation cost in decryption. Later, Phuong et al. [48] designed an efficienty fully hidden policy CP-ABE scheme, while it only supports restricted access policy. Recently, the studies in [15], [49], [50] developed several CP-ABE schemes that supports fully hidden and expressive access policy, but it lacks support for large attribute universe.

In Table I, we compare our proposed scheme, i.e, TAHP-CP-ABE, with several existing state-of-the-art schemes from various propoerties including policy hiding, large universe, time limited data access control, full security, standard model, online/offline encryption, outsourced decryption, data auditing.

TABLE I
FUNCTION COMPARISON IN VARIOUS SCHEMES

| Scheme | PH | LU | TLDAC | FS | SM | OOE | DT | Data Auditing |
|---|---|---|---|---|---|---|---|---|
| Scheme [13] | ✓ | × | × | ✓ | × | × | × | × |
| Scheme [30] | ✓ | × | × | ✓ | × | ✓ | × | × |
| Scheme [32] | × | ✓ | × | ✓ | × | ✓ | × | × |
| Scheme [40] | ✓ | × | × | ✓ | × | × | × | × |
| Scheme [7] | × | ✓ | × | ✓ | ✓ | × | ✓ | × |
| Scheme [44] | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | × |
| Scheme [43] | ✓ | ✓ | × | × | × | × | × | × |
| Scheme [15] | × | ✓ | ✓ | × | × | × | × | ✓ |
| **TAHP-CP-ABE** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**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.

## III. PRELIMINARIES

In this section, we provide several concepts and definitions used in our proposal including access structure, composite bilinear maps.

### A. Access Structure

***Definition** 1:* (Access Structure [51]). Let $\{Q_1, \cdots, Q_n\}$ be a set of parties. A collection $C \subseteq 2^{\{Q_1,\cdots,Q_n\}}$ is monotone if $\forall H, I$ : if $H \in C$ and $H \subseteq I$, then $I \in C$. An access structure $S$ has nonempty subsets of $\{Q_1, \cdots, Q_n\}$. Authorized sets are the sets in $S$ and others are unauthorized sets. Moreover, each user corresponds with an attribute set and we regard a user as authorized if his attribute set is involved in $S$.

### B. Linear Secret Sharing Schemes (LSSS)

***Definition** 2:* (LSSS [25]). Given the attribute universe $U_a$, an LSSS on it involves $(B, \delta)$, where $B$ is an $l \times n$ share-generating matrix on $Z_p$ and the function $\delta$ maps a row of $B$ into an attribute in $U_a$. There are two algorithms: Share and Reconstruction in an LSSS. The former is to create the shares for a secret value $s$ based on $B$ with $\bar{b} = (s, b_2, \cdots, b_n)^T$, where $b_2, \cdots, b_n {\in_R} Z_p$ by $\lambda_x = B_x \cdot \bar{b}$ as a share of the secret $s$, while the latter reconstructs $s$ with the secret shares of an authorized set $E$ by finding $I = \{i|\delta(i) \in E\} \subseteq \{1, 2, \cdots l\}$ and constances $\omega_i \in Z_p$ to make $\sum_{i\in I} w_i B_i = (1, 0, \cdots, 0)$ hold and compute $\sum_{i\in I} w_i \lambda_i = s$.

### C. Bilinear Map

***Definition** 3:* (Bilinear Map [52]). We consider two multiplicative cyclic groups $G$ and $G^{'}$ under prime order $p$ and a generator $g$ in group $G$. Let $\hat{e}\colon G \times G \rightarrow G^{'}$ a bilinear map if it satisfies the following features:

1) Bilinearity: $\hat{e}(g_1^v, g_2^f) = \hat{e}(g_1, g_2)^{vf} \quad for \quad \forall \quad v, f \in Z_p \quad and \quad g_1, g_2 \in G$.
2) Non-Degeneracy: $\hat{e}(g_1, g_1) \neq 1$.
3) Computability: $\hat{e}(d, f)$ can be computed efficiently for $\forall d, f \in G$.

## IV. SYSTEM MODEL AND DESIGN GOALS

In this section, we show the system model and design goals of our TAHP-CP-ABE.

### A. System Model

In the system model of our proposed TAHP-CP-ABE, there mainly are four entities, that is, Trusted Authority (TA), Industrial Cloud Provider (ICP), Data Owner (DO) and Data User (DU). The detailed description of each entity is listed as follows.

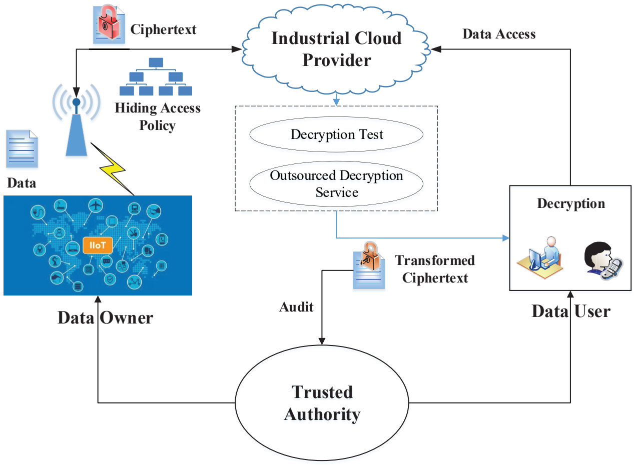


Fig. 1. The system model of TAHP-CP-ABE

- TA is in charge of initializing the whole system by generating various required parameters and its master key. Moreover, TA also takes charge of user registration when a new user takes part in the system. Besides, TA supports data auditing for DU when they receive transformed ciphertexts from ICP.
- ICP is the provider that eliminates the local burden of users by providing them with sufficient storage and computation resources and various services of cloud including data storage, sharing and outsourced decryption after validating their access permission.
- DO is the owner of IIoT devices deployed ubiquitously in everywhere of industrial sectors to collect important

data for analysis and monitoring. To eliminate the heavy storage and computing burden of these resource-limited IIoT devices, DO encrypts the data and uploads to cloud. Thus, the IIoT data can be shared by relevant users through cloud data sharing services.

- DU is the consumer of IIoT data. To obtain the shared IIoT data, DU issues a data access request to ICP for required data. After the access times and permission verification for the DU, ICP finishes outsourced decryption and returns the transformed ciphertext back to DU. Then ,DU can recover the plaintext data and conducts data auditing by interacting with TA.

### B. Threat Model

In our TAHP-CP-ABE, we assume that ICP is a semi-trusted entity, that is, it honestly obeys the pre-defined protocol in runtime applications while gets curious about the data stored in it or transmitted between ICP and DU. Moreover, in the provision of outsourced decryption, ICP is untrusted if lazily or maliciously returns false results to DU. TA and DO are considered as honest and trusted as the former is used to initiate and manage the whole system while the latter aims to outsoure and share their own data to cloud. DU is deemed as a untrusted entity as part of DUs may intentionally spy on the private information in exposed access policies and the data between a honest DU and ICP, or even maliciously obtains the shared data by colluding or exhaustive guessing attacks.

### C. Design Goals

To address the above threats and corresponding challenging problems, we propose TAHP-CP-ABE to guarantee the privacy protection, fine-grained access control and limited access times for the shared IIoT data in ICP while achieving high efficiency in practice. Specifically, we have the following design goals:

- Fine-grained access control: The shared IIoT data in ICP should be shared or accessed by only specific DUs with enough privilege. Also, the IIoT data is expected to be shared or accessed within limited times to prevent attacks by unlimited illegal data access.
- Attribute Privacy Preserving: In TAHP-CP-ABE, those sensitive or privacy-aware attribute values associated with access policies need to be hidden in encrypted IIoT data for privacy preserving.
- Efficiency: For the sake of resource-limited IIoT devices for industrial sectors, it is preferable for ICP to efficiently check user permission and access times before data decryption and for DU to outsource the high computational burden in decryption to ICP.

### D. Security Model

In this part, we present the security model for TAHP-CP-ABE by designing a security game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$ described as follows.

- *Setup*: The challenger $\mathcal{B}$ initializes the system and generates the system public parameters $PK$ and master key $MSK$. It then sends the $PK$ to the adversary $\mathcal{A}$.
- *Phase 1*: The adversary $\mathcal{A}$ issues a series of queries $q_1, \cdots, q_n$ adaptively, where $n$ is a polynomially bounded number and $q_i$ may be one kind of the following queries:
  - *UKey Query*: The adversary $\mathcal{A}$ requests his secret key by submitting an attribute set $\mathcal{S}$ and an identity $uid^{'}$ to the challenger $\mathcal{B}$. The challenger runs $KeyGen_U$ and returns the $sk_{uid,\mathcal{S}}$ to the adversary $\mathcal{A}$.
  - *OKey Query*: The adversary $\mathcal{A}$ launches transformation key queries with an attribute set $\mathcal{S}$ and an identity $uid^{'}$ to the challenger $\mathcal{B}$. The challenger runs $KeyGen_{OUT}$ and returns the $TK$ to the adversary $\mathcal{A}$.
- *Challenge*: The adversary $\mathcal{A}$ ends the *Phase 1* and submits two equal length messages $m_0$ and $m_1$ with two access policy $\mathcal{A}_0, \mathcal{A}_1$ and a revocation list $RL^*$. Then, the challenger $\mathcal{B}$ randomly chooses $u \in [0,1]$, encrypts $m_u^{'}$ and returns the ciphertext $CT^{'}$ to $\mathcal{A}$.
- *Phase 2*: The adversary $\mathcal{A}$ repeats the *Phase 1* and the queries with submitted attribute set $\mathcal{S}$ and identity $uid^{'}$ that none of the queried attribute sets satisfies $\mathcal{A}_0, \mathcal{A}_1$ and $uid \notin RL^*$.
- *Guess*: The adversary $\mathcal{A}$ outputs a bit $u^{'} \in [0,1]$. If $u^{'} = u$, $\mathcal{A}$ wins the game. The advantage of $\mathcal{A}$ is defined as $Adv_{\mathcal{A}} = |Pr[u^{'} = u] - \frac{1}{2}|$.

***Definition 4:*** The TAHP-CP-ABE scheme is indistinguishable under chosen-plaintext attacks if there exists a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ that can win the game with non-negligible advantage $Adv_{\mathcal{A}}$.

## V. Construction of TAHP-CP-ABE

In this section, before introducing the construction of our TAHP-CP-ABE, we first give the definition of some notations utilized in our proposal in Table II as well as its workflow in practical deployment.

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 $S$.

TABLE II
Notation Descriptions in HMGDSF

| Notations | Descriptions |
|---|---|
| $S_u$ | attribute set of a DU |
| $U_a$ | attribute universe of the system |
| $PK, MSK$ | system public parameter and master key |
| $PK_u, SK_u$ | public and secret keys of DU |
| $SK_a, TK_u$ | decryption key and transformation key of DU |
| $IT_t, CT$ | intermediate ciphertext, resultant ciphertext |
| $CT^{'}$ | transformed ciphertext |

### A. Overview of the workflow

TAHP-CP-ABE is proposed to guarantee fine-grained data access control for data sharing service of Cloud-assisted IIoT applications. Besides, it also aims to provide privacy preservation for access policies and the limitation over access times. Fig.2 shows the workflow of TAHP-CP-ABE in practice. As we can see, TAHP-CP-ABE includes three phases in runtime,

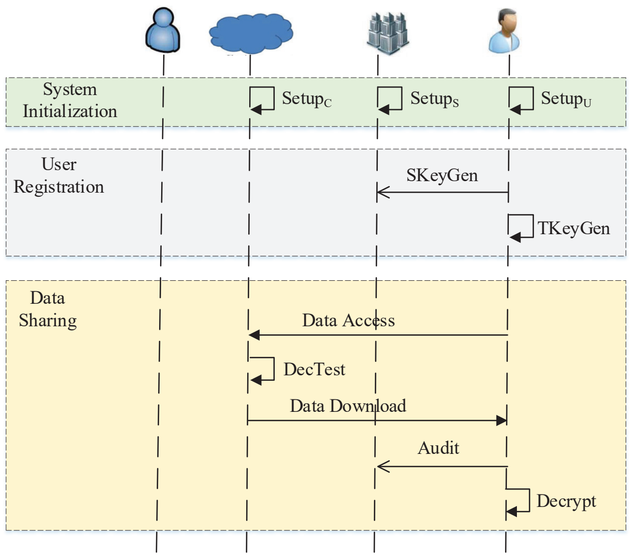


Fig. 2. The workflow of TAHP-CP-ABE

that is, system initialization phase, user registration phase and data sharing phase.

Specifically, as shown in Fig.2, in system initialization phase, TA initiates the whole system in the meantime ICP and each DU initialize their own parameters. When a DU intends to take part in the system, he needs to register to TA, which opens up the user registration phase. Then, if a DU aims to conduct data access operations in order to share the data of IIoT, comes with the data sharing phase. In this phase, DO first uploads the ciphertext to ICP for data sahring. After receiving the data access request from DU, ICP first checks if the attribute set of the DU matches the shared data. To resist DoS attacks, ICP also has to verify the accumulative access times of the DU. If the access times does not exceeds the maximum, the data access phase continues, otherwise, the phase aborts. If the request passes these verification, ICP executes outsourced decryption to eliminate the workload of resource-limited devices owned by DU. When DU recieves the transformed ciphertext, to prevent probabily lazy outsourced decryption of ICP, DU can audit the results by interacting with TA for data audiging.

### B. Concrete Construction

Subsequently, we present the detailed construction of our proposal.

#### 1) System Initialization Phase

In this phase, TA generates the system master key and public parameters to initiate the whole system. ICP and each DU also finish their own setup.

- $Setup_S(\lambda)$: After taking the security parameter $\lambda$, TA begins to initialize the whole system.
  - TA generates a bilinear group with composite order $N$, that is, $(N, p_1, p_2, p_3, p_4, G_0, G_t, \hat{e})$, where $N = p_1 p_2 p_3 p_4$ and $p_1, p_2, p_3, p_4$ are four different prime numbers. TA takes $Z_N$ as the attribute universe, that is, $U_a = Z_N$ which is a large attribute universe.
  - TA uniformly chooses $\alpha, a \in_R Z_N, g, h \in_R Z_N, X_3 \in_R G_{p_3}, Z, X_4 \in_R G_{p_4}$ to compute $E = \hat{e}(g, g), Y = E^{\alpha}, H = hZ$.
  - TA picks a collision resistant hash function $H_m : \{0,1\}^* \to Z_N$.
  - TA generates the system master key $MSK = \{\alpha, h, X_3\}$ and outputs the system public parameter $PK = \{N, g, g^a, Y, H, X_4, H_m, E\}$.
- $Setup_C(PK)$: After the system initalization of TA, ICP gets the system public parameter $PK$ and initiates the counter as $ctr = 0$ for outsourced decryption service. For each transformation key, ICP generates an empty set $ST$ and a list $L_k$ to keep $ctr$ and $ST$.
- $Setup_U(PK)$: After the system initalization of TA, each DU chooses $\mu_u \in_R Z_N$ as the private key, i.e., $SK_u = \mu_u$ and generates corresponding public key $PK_u = g^{\mu_u}$. Finally, DU outputs his public key $PK_u$.

#### 2) User Registration Phase

In this phase, users of IIoT applications take part in the system and register themselves to TA for key distribution.

- $SKeyGen(PK, MSK, S_u, PK_u)$: When a DU with attribute set $S_u$ and public key $PK_u$ requests to register himself in the system, where $S_u = (I_s, \overline{S}_u)$ and $I_s \subset Z_N, \overline{S}_u = \{a_i\}_{i \in I_s}$, TA uniformly chooses $t_u \in_R Z_N$ and for each $i \in I_s$, it selects $R, R^{'}, R_i \in_R G_{p_3}$. Then, TA generates the secret key for DU as $SK_a = \{S_u, K, K^{'}, \{K_i\}_{i \in I_s}\}$, where

  $$K = PK_u^{\alpha} g^{a t_u} R, K^{'} = g^{t_u} R^{'},$$
  $$\forall i \in I_s : K_i = (g^{a_i} h)^{t_u} R_i$$

  **Note**. As the component $K$ is related to the public key $PK_u$ of each DU, in decryption phase, only the correct DU that holding corresponding private key $SK_u$ can decrypt the ciphertext. As a result, the public key $PK_u$ can be used for data auditing with partial decryption result without introducing extra ciphertext component for verifiability as in scheme [14]. The detailed description is shown in *Audit* algorithm.
- $TKeyGen(PK, SK_a, csi)$: After receiving the secret key $SK_a$, with the system information $csi$ generated by TA, the DU computes $K_c = E^{1/(\mu_u + H_m(csi))}, K_p = g^{1/(\mu_u + H_m(csi))}$ and outputs his transformation key $TK_u = (SK_a, K_c, K_p, csi)$.

#### 3) Data Sharing Phase

In this phase, DO uploads the encrypted IIoT data to ICP for outsourcing and sharing, while DU issues data access request and obtains the requierd dta if authorized and honest.

- $Encrypt_{off}(PK) \to IT_t$: Given the system public key $PK$, each DO prepares the encryption process in advance. DO selects random values $s, s^{'} \in Z_N$ as secret value for sharing to compute $\widetilde{C}_{\delta}^{'} = Y^{s^{'}}, \widetilde{C}_1^{'} = Y^{s}, \widehat{C}_{\delta}^{'} = g^{s^{'}}, \widehat{C}_1^{'} = g^{s}$ and constructs a intermediary pool $IT_1 = \{(s, s^{'}, \widetilde{C}_{\delta}^{'}, \widetilde{C}_1^{'}, \widehat{C}_{\delta}^{'}, \widehat{C}_1^{'})\}$. Then, DO chooses $\lambda^{'}, t^{'}, r^{'} \in_R Z_N$ and calculates $C_{\delta,x}^{'} = g^{a\lambda^{'}}, C_{1,x}^{'} = g^{a\lambda^{'}} (g^{t^{'}} H)^{r^{'}}, C_{2,x}^{'} = g^{r^{'}}$ to construct another intermediary pool $IT_2 = \{(\lambda^{'}, t^{'}, r^{'}, C^{'}_{\delta,x}, C^{'}_{1,x}, C^{'}_{2,x})\}$. Finally, DO 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 IIoT 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 $\mathcal{A}$, DO 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. DO 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, DO 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, DO 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

$$\widetilde{C_\delta} = \widetilde{C_\delta}^{'}, \widehat{C_\delta} = \widehat{C_\delta}^{'} \cdot O_\delta,$$
$$C_{\delta,x} = C^{'}_{\delta,x} \cdot (g^{t_{\rho(x)}} H)^{-s^{'}} O_{c,x},$$
$$\widetilde{C_1} = M \cdot \widetilde{C_1}^{'}, \widehat{C_1} = \widehat{C_1}^{'},$$
$$C_{1,x} = C^{'}_{1,x} \cdot O_{c,x}, C_{2,x} = C^{'}_{2,x} \cdot O_{d,x},$$
$$C_{3,x} = A_x \cdot v - \lambda^{'}_x, C_{4,x} = A_x \cdot v^{'} - \lambda^{'}_x,$$
$$C_{5,x} = r^{'}_x (t_{\rho(x)} - t^{'}_x)$$

  Finally, DO uploads the ciphertext $CT$ to ICP for data outsourcing and sharing.

- $DecTest(PK, CT, S_u, TK_u)$: When a DU wants to request shared IIoT data to ICP. he sends a data access request to ICP with his transformation key $TK_u$, ICP executes the following steps for decryption test to verify if the DU has enough permission for data sharing.
  - After receiving the system public key $PK$ and the IIoT data access request from DU with his transformation key $TK_u$, ICP first checks if the access time of the DU reach the maximum as follows:
    1) $\hat{e}(g^{H_m(csi)} \cdot PK_u, K_p) = E$ and $K_c = \hat{e}(g \cdot PK_u, K_p)$;
    2) $ctr + 1 \leq \varepsilon$, where $\varepsilon$ is the maximum access time of the outsourced decryption service request for IIoT data sharing;
    3) $K_c \notin ST$.

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

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

    Then, ICP allows the DU to download the ciphertext $CT$ and returns the transformed ciphertext $CT^{'} = ((A, \rho), C^{'})$ of the shared IIoT data to DU.

- $Decrypt(CT^{'}, SK_u)$: On inputting the transformed ciphertext $CT^{'} = ((A, \rho), C^{'})$ and the user private key $SK_u = \mu_u$, the DU calculates the message plaintext as following:

$$CF^{'} = C^{'} / \hat{e}(g^{-SK_u}, \widehat{C}_1) = Y^s, M = \widetilde{C}_1 / CF^{'}$$

  Then, DU can get the plaintext data as $M$.

- $Audit(PK, MSK, PK_u, CF)$: Given the transformed ciphertext $CF$, TA utilizes the system master key and public parameter to check the correctness of $CF$ by following equation:

$$\hat{e}(PK_u \cdot g^{\alpha}, \widehat{C}_1) = C^{'}$$

  If the above equation holds, the ICP executes the outsourced decryption honestly. Otherwise, the transformed ciphertext $CF$ is not correct.

## VI. Analysis of TAHP-CP-ABE

### A. Security Analysis

***Theorem 1:*** Our TAHP-CP-ABE scheme is fully secure under our security model if the PASH scheme in [7] is fully secure.

***Proof 1:*** As we also adopt the similar hybrid encryption mechanism as in [7], the security of our scheme can be reduced to that of PASH. If the adversary $\mathcal{A}$ can break the our scheme with non-negligible advantage $Adv_0 = \epsilon$, then we can construct a simulator $\mathcal{C}$ that can break the PASH scheme $Adv_1$ which is identical to $Adv_0$.

- *Setup*: The simulator $\mathcal{C}$ initializes the PASH scheme and generates the system public parameters $PP_{PASH} = \{N, g, g^\alpha, H, Y, X_4\}$ and master key $MSK_{PASH} = \{\alpha, h, X_3\}$. After gets the $PP_{PASH}$, the challenger $\mathcal{B}$ of our TAHP-CP-ABE scheme initializes generates $PP_{TAHP-CP-ABE} = \{N, g, g^\alpha, \gamma, \theta, g^a, g^b, g^c, H, Y, X_4\}$ and $MSK_{TAHP-CP-ABE} = \{\alpha, h, X_3\}$. The challenger $\mathcal{B}$ also initializes a full binary tree $T_u$ for the user identity universe.
- *Phase 1*: The adversary $\mathcal{A}$ queries secret key with an attribute set $\mathcal{S}$ and identity $uid$. $\mathcal{C}$ returns the secret key $sk_{\mathcal{S}} = \{\mathcal{S}, K, K^{'}, \{K_i\}_{i \in I_{\mathcal{S}}}\}$, where $K = g^\alpha g^{at} R, K^{'} = g^t R^{'}, K_i = (g^{s_i} h)^t R_i$. Then, the challenger $\mathcal{B}$ randomly selects $u, u^{'} \in Z_N, R_2, R_3 \in G_{p_3}$, and computes $sk_{uid,\mathcal{S}}$ as follows:

$$\begin{aligned} &K_{1,\varepsilon_i} = g^\alpha g^{at} g^{bu} g^{cu^{'} H_1(\varepsilon_i)} R, \\ &K_2 = g_1^u R_2, K_3 = g_1^{u^{'}} R_3, K_4 = g^t R^{'}, \\ &K_{5,x} = (g^{s_x} h)^t R_x, \end{aligned} \tag{1}$$

  Then, the challenger $\mathcal{B}$ returns $sk_{uid,\mathcal{S}}$ to $\mathcal{A}$.
- *Challenge*: The adversary $\mathcal{A}$ submits two messages $m_0, m_1$ with equal length and two challenge access policies $\mathcal{A}_0 = (A, \rho, R_{A0}), \mathcal{A}_1 = (A, \rho, R_{A1})$ and a revocation list $RL^*$ to $\mathcal{B}$. The simulator $\mathcal{C}$ randomly chooses $u \in [0, 1]$ and returns the ciphertext $C = m_u \cdot Y^s, C_0 = g^s, C_x = g^{aA_x \cdot v} (g^{t_{\rho(x)}} H)^{-r_x} W_{x,1}, D_x = g^{r_x} W_{x,2}, \overline{C} =$

$Y^{s'}, \overline{C}_0 = g^{s'}\overline{W}, \overline{C}_x = g^{aA_x \cdot v'}(g^{t_{\rho(x)}}H)^{-s'}\overline{W}_x$ with access policy $\mathcal{A}_u$. Then, $\mathcal{B}$ computes the following $CT_{\mathcal{A}_u}$:

$$\begin{aligned}
&C_{2,\varepsilon_i} = (g_1^{cH_1(\varepsilon_i)})^s H_{2,\varepsilon_i}, C_{3,x} = C_x, C_{4,x} = D_x,\\
&\overline{C} = \overline{C}, \overline{C_0} = \overline{C}_0, \overline{C_1} = (\overline{C}_0)^b \overline{H_1},\\
&\overline{C_{2,\varepsilon_i}} = (\overline{C}_0)^{cH_1(\varepsilon_i)}\overline{H_{2,\varepsilon_i}}, \overline{C_{3,x}} = \overline{C}_x\overline{H_{3,x}},
\end{aligned}$$

- *Phase 2*: The adversary $\mathcal{A}$ repeats the queries as *Phase 1* and none of the queried attribute sets satisfies $\mathcal{A}_0, \mathcal{A}_1$ and $uid \notin RL^*$.
- *Guess*: The adversary $\mathcal{A}$ guass the $u'$ and returns to challenger $\mathcal{B}$. If $u' = u$, $\mathcal{A}$ wins the security game of our scheme, then $\mathcal{C}$ can break the security game of PASH scheme and the security of our scheme reduces to that of PASH. The advantage of $\mathcal{A}$ to break our scheme is identical to that of $\mathcal{C}$ to break PASH.

  In conclusion, if PASH is fully secure, our TAHP-CP-ABE is fully secure in standard model.

Moreover, in our scheme, we highlight the privacy protection of attributes in cloud-assisted IIoT system. From the above construction of scheme, we infer that the attribute values are encrypted with IIoT ciphertext, and the attribute name remains in access structure $(A, \rho)$. Thus, the curious ECP cannot get any information about IIoT data from access policies.

### *B. Performance Analysis*

In this section, we analyze the performance of our TAHP-CP-ABE from theoretical and practical point of view by comparing two existing state-of-the-art schemes, i.e, PASH [7], HTAC [44] and PH-LU-CPABE [43]. In theoretical analysis, the size of public parameters are denoted by $PPSize$, while the size of decryption key by $DKSize$ and the size of ciphertext by $CTSize$, respectively. Note that the users are resource-limited. We will highlight the complexity of algorithms in user side or executed by IIoT devices. We take $P$ for bilinear pairing operation, $E$ for exponentiation operation in $G$, and $ET$ for exponentiation operation in $G_T$, respectively. Moreover, we represent the size of the attribute universe with $N$, the number of a user's attributes with $|S|$, the number of rows in a policy generation matrix with $l$ and the size of minimum authorized set $I$ as $|I|$.

From Table III, we can infer that, comparing with PASH, HTAC and PH-LU-CPABE, the time cost of secret key generation in our scheme is the same with that of PASH and PH-LU-CPABE while less than that of HTAC which costs more time for user tracing. Moreover, TAHP-CP-ABE costs much less computation than the other three schemes in encryption as it achieves online/offline encryption by move a majority of computation to offline phase . In decryption phase, in TAHP-CP-ABE, the computation complexity is largely reduced compared with the other two schemes. The improvement here is that we use outsourced decryption after decryption test, which can reduce the user side computation complexity in IIoT device. From Table IV, it is obvious that TAHP-CP-ABE costs the same storage for public parameter as PASH and PH-LU-CPABE while has less storage than that of HTAC which costs one more elements of $G$ for user tracing. For the same reason, the storage cost of user secret key in TAHP-CP-ABE is also the same as that of PASH while less than that of HTAC and PH-LU-CPABE. However, as our scheme introduces online/offline encryption, it takes more storage cost for extra components in ciphertext.

To evaluate the practical performance of TAHP-CP-ABE, we implement a prototype of it using Java language and JPBC lib [53]. We adopt the Type A curve to realize the bilinear group and various operations. For comparison, we also implement PASH, HTAC and PH-LU-CPABE in the same way within same settings. In our experiments, we set the size of attribute universe in the range of $|U| \in [5, 50]$ to evaluate the public parameter size and the size of attribute set $|S|$ is in the range of $[5, 50]$ for the evaluation of the time and storage cost of key generation. To assess the time and storage cost of encryption, we let the row number of access policy $l$ range from 10 to 50, while for the time cost of decryption assessment, the complexity of access policy $|I|$ is ranging in $[5, 10, 15, 20]$ with the number of files ranging in $[5, 10, 15, 20]$. Then, we show the performance evaluation comparison in Fig.3.

In Fig.3(a) and Fig.3(b), we notice that the time cost of user secret key generation in TAHP-CP-ABE is similar to that of PASH, HTAC and PH-LU-CPABE, while the storage cost of the user secret key in TAHP-CP-ABE and PASH is a bit less than that of HTAC and PH-LU-CPABE. The reason in that the latter two schemes cost more storage of user secret key for user tracing.

Fig.3(c) and Fig.3(d) show the time cost and storage cost of encryption algorithm. It is obvious that the time cost of data encryption in TAHP-CP-ABE is much less than that of PASH, HTAC and PH-LU-CPABE by levaraging online/offline encryption technique. Whereas, the storage cost of ciphertext in TAHP-CP-ABE is more than that of the other three schemes for the reason that it needs extra ciphertext component for the introduction of online/offline encryption. However, it is preferable for resource-limted IIoT devices, as the ciphertext is stored in cloud.

We depict the performance evaluation of decryption and public parameters in Fig.3(e) and Fig.3(f), respectively. It is worthy noticing that the time cost of user decryption in TAHP-CP-ABE is much less than that of the other three schemes with the help of outsourced decryption. What is more, the storage cost for public parameter in TAHP-CP-ABE is the same as that of PASH and PH-LU-CPABE while less than that of HTAC which takes more parameters for user tracing.

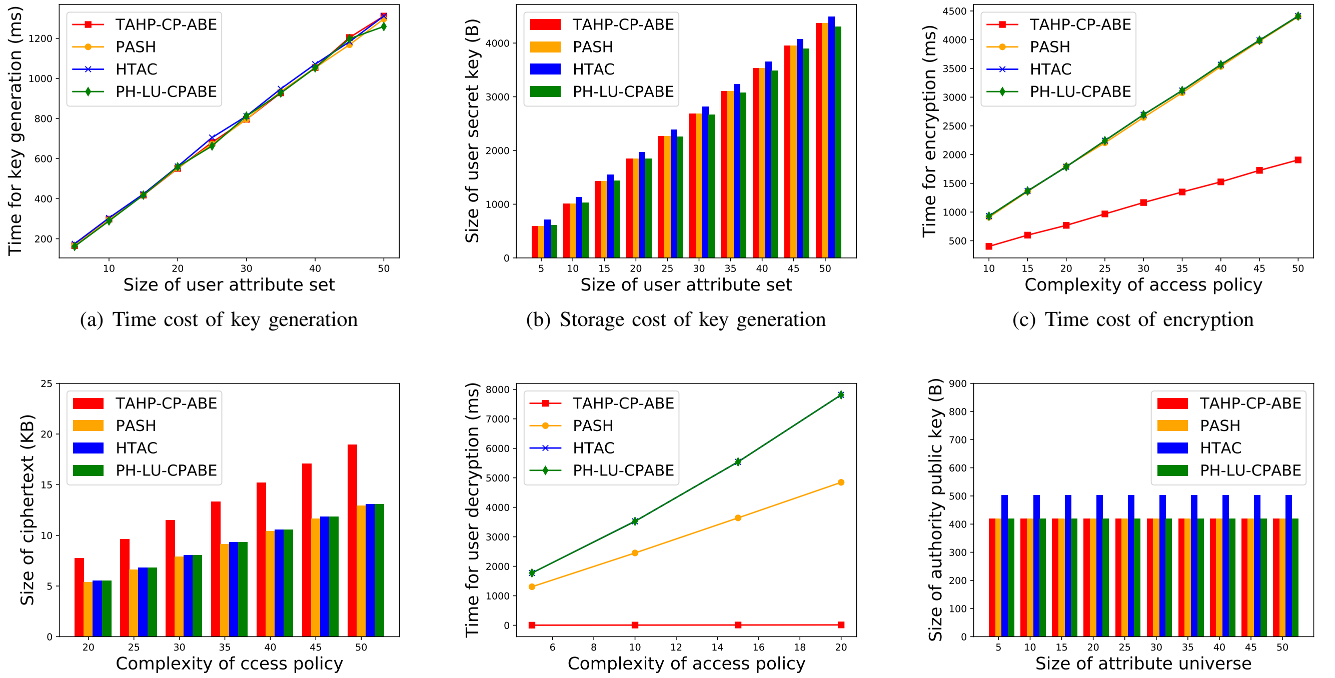
Above all, the theoretical analysis of TAHP-CP-ABE is consistant with the practical performance analysis. Specifically, TAHP-CP-ABE has a superior performance compared to PASH and HTAC in both encryption and decryption, except that it cost a bit more storage for ciphertext. Nevertheless, the ciphertex is stored in cloud and thus has no effect on IIoT devices. Moreover, TAHP-CP-ABE achieves access times limitation, large universe, data auditing and policy hiding at the same time. As a result, TAHP-CP-ABE is more practical in Cloud-based IIoT application.

TABLE III
COMPUTATION COST COMPARISON

| Schemes | KeyGen | UserEnc | UserDec |
|---|---|---|---|
| PASH | $(2\|S\|+3)E$ | $(7l+4)E+2E_T$ | $2\|I\|E+(\|I\|+1)E_T+(2\|I\|+3)P$ |
| HTAC | $(2\|S\|+4)E$ | $(7l+5)E+2E_T$ | $(3\|I\|+4)E+(\|I\|+1)E_T+(2\|I\|+4)P$ |
| PH-LU-CPABE | $(2\|S\|+3)E$ | $(6l+2)E+2E_T$ | $(4\|I\|+2)E+4P$ |
| TAHP-CP-ABE | $(2\|S\|+3)E$ | $2lE$ | $E$ |

TABLE IV
STORAGE COST COMPARISON

| Schemes | PPSize | DKSize | CTSize |
|---|---|---|---|
| PASH | $4\|G_{p_i}\|+\|G_T\|$ | $(\|S\|+2)\|G_{p_ip_j}\|$ | $(2l+3)\|G_{p_ip_j}\|+2\|G_T\|$ |
| HTAC | $5\|G_{p_i}\|+\|G_T\|$ | $(\|S\|+3)\|G_{p_ip_j}\|+\|Z_N\|$ | $(3l+4)\|G_{p_ip_j}\|+2\|G_T\|$ |
| PH-LU-CPABE | $4\|G_{p_i}\|+\|G_T\|$ | $(\|S\|+2)\|G_{p_ip_j}\|+\|Z_N\|$ | $(2l+2)\|G_{p_ip_j}\|+2\|G_T\|$ |
| TAHP-CP-ABE | $4\|G_{p_i}\|+\|G_T\|$ | $(\|S\|+2)\|G_{p_ip_j}\|$ | $(2l+3)\|G_{p_ip_j}\|+2\|G_T\|+3l\|Z_N\|$ |



(a) Time cost of key generation

(b) Storage cost of key generation

(c) Time cost of encryption

(d) Storage cost of encryption

(e) Time cost of decryption

(f) Storage cost of system public parameter

Fig. 3. Performance evaluation of TAHP-CP-ABE

## VII. CONCLUSION

In this paper, facing the severe data security problems in cloud-assisted IIoT data sharing scenario, we proposed a k-Times and auditable hidden-policy CP-ABE scheme, that is, TAHP-CP-ABE as a countermeasure. The proposed scheme can achieve fine-grained data access control by inheriting the property from standard CP-ABE and privacy leakage resistance in access policy using the policy hiding technique for shared IIoT data in cloud. In addition, in order to limit the access times for special data user, we utilizing the time-limit technique and realize the access time limitation. Moreover, for resource-limited users, we use the decryption test and decryption outsourcing techniques to move a majority of complex computation burden of data decryption to cloud. Last but not the least, analysis and experimental results indicate that TAHP-CP-ABE is fully secure in standard model and efficient than existing related schemes.

In the next step, we will study the public traceability in data sharing service of cloud-assisted industrial Internet of Things to prevent the key leakage and abuse problem.

## ACKNOWLEDGMENT

This research is funded by National Natural Science Foundation of China (No. 61902291), China Postdoctoral Science Foundation Funded Project(2019M653567), the Fundamental Research Funds for the Central Universities (XJS211516), R&D Program of Shaanxi Province (No. 2019ZDLGY12-03).

## References

[1] Lv, Z., Qiao, L., Li, J., Song, H.: Deep-learning-enabled security issues in the internet of things. IEEE Internet of Things Journal **8**(12), 9531–9538 (2020)

[2] Wei, W., Yang, R., Gu, H., Zhao, W., Chen, C., Wan, S.: Multi-objective optimization for resource allocation in vehicular cloud computing networks. IEEE Transactions on Intelligent Transportation Systems (2021)

[3] Qi, S., Lu, Y., Wei, W., Chen, X.: Efficient data access control with fine-grained data protection in cloud-assisted iiot. IEEE Internet of Things Journal **8**(4), 2886–2899 (2020)

[4] Jiang, S., Cao, J., Wu, H., Yang, Y.: Fairness-based packing of industrial iot data in permissioned blockchains. IEEE Transactions on Industrial Informatics (2020)

[5] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2005, pp. 457–473.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006, pp. 89–98.

[7] Zhang, Y., Zheng, D., Deng, R.H.: Security and privacy in smart health: Efficient policy-hiding attribute-based access control. IEEE Internet of Things Journal **5**(3), 2130–2145 (2018)

[8] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling efficient data sharing with auditable user revocation for iov systems," *IEEE Systems Journal*, 2021.

[9] Xu, Y., Deng, G., Zhang, T., Qiu, H., Bao, Y.: Novel denial-of-service attacks against cloud-based multi-robot systems. Information Sciences **576**, 329–344 (2021)

[10] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," pp. 162–179, 2013.

[11] K. Yang and X. Jia, "Attributed-based access control for multi-authority systems in cloud storage," pp. 536–545, 2012.

[12] M. Green, S. Hohenberger, B. Waters *et al.*, "Outsourcing the decryption of abe ciphertexts." in *USENIX Security Symposium*, vol. 2011, no. 3, 2011.

[13] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343–1354, 2013.

[14] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 7, pp. 1384–1393, 2015.

[15] Ning, J., Cao, Z., Dong, X., Liang, K., Ma, H., Wei, L.: Auditable \ $\sigma$ -time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security **13**(1), 94–105 (2017)

[16] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE transactions on dependable and secure computing*, vol. 15, no. 4, pp. 708–722, 2016.

[17] Z. Li, D. Wang, and E. Morais, "Quantum-safe round-optimal password authentication for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.

[18] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, 2020.

[19] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, 2020.

[20] Jiang, Q., Zhang, X., Zhang, N., Tian, Y., Ma, X., Ma, J.: Three-factor authentication protocol using physical unclonable function for iov. Computer Communications **173**, 45–55 (2021)

[21] Zhao, G., Jiang, Q., Huang, X., Ma, X., Tian, Y., Ma, J.: Secure and usable handshake based pairing for wrist-worn smart devices on different users. Mobile Networks and Applications pp. 1–16 (2021)

[22] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," pp. 463–474, 2013.

[23] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on bpv-fourq for internet of drones," *Peer-to-Peer Networking and Applications*, pp. 1–14, 2021.

[24] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[25] J. Zhang, J. Ma, Z. Ma, N. Lu, Y. Yang, T. Li, and D. Wei, "Efficient hierarchical data access control for resource-limited users in cloud-based e-health," in *2019 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2019, pp. 319–324.

[26] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*. IEEE, 2007, pp. 321–334.

[27] F. Guo, Y. Mu, and Z. Chen, "Identity-based online/offline encryption," *Lecture Notes in Computer Science*, vol. 5143, pp. 247–261, 2008.

[28] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," *Journal of Cryptology*, vol. 9, no. 1, pp. 35–67, 1996.

[29] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," pp. 355–367, 2001.

[30] Hohenberger, S., Waters, B.: Online/offline attribute-based encryption. In: International workshop on public key cryptography. pp. 293–310. Springer (2014)

[31] P. Datta, R. Dutta, and S. Mukhopadhyay, "Fully secure online/offline predicate and attribute-based encryption," *International Conference on Information Security Practice and Experience*, pp. 331–345, 2015.

[32] De, S.J., Ruj, S.: Efficient decentralized attribute based access control for mobile clouds. IEEE Transactions on Cloud Computing **8**(01), 124–137 (2020)

[33] H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," *IEEE transactions on dependable and secure computing*, vol. 14, no. 6, pp. 679–692, 2017.

[34] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1735–1744, 2014.

[35] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," *IEEE Access*, vol. 7, pp. 102 887–102 901, 2019.

[36] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "Fadb: A fine-grained access control scheme for vanet data based on blockchain," *IEEE Access*, vol. 8, pp. 85 190–85 203, 2020.

[37] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, "Trustaccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.

[38] H. Cui, Z. Wan, X. Wei, S. Nepal, and X. Yi, "Pay as you decrypt: Decryption outsourcing for functional encryption using blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3227–3238, 2020.

[39] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," *International conference on applied cryptography and network security*, pp. 111–129, 2008.

[40] J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," *Proceedings of the 7th ACM symposium on information, computer and communications security*, pp. 18–19, 2012.

[41] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding cp-abe," *International conference on information security practice and experience*, vol. 6672, pp. 24–39, 2011.

[42] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, "Anonymous attribute-based encryption supporting efficient decryption test," pp. 511–516, 2013.

[43] 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 Journal (2021)

[44] 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), 1–1 (2020)

[45] H. Cui, R. H. Deng, G. Wu, and J. Lai, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures," vol. 10005, pp. 19–38, 2016.

[46] H. Cui, R. H. Deng, J. Lai, X. Yi, and S. Nepal, "An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited," *Computer Networks*, vol. 133, pp. 157–165, 2018.

[47] Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 126–138, 2015.

[48] T. V. X. Phuong, G. Yang, and W. Susilo, "Hidden ciphertext policy attribute-based encryption under standard assumptions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 35–45, 2016.

[49] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, “Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot,” *Computer Networks*, vol. 133, pp. 141–156, 2018.

[50] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, “Efficient and privacy preserving access control scheme for fog-enabled iot,” *Future Generation Computer Systems*, vol. 99, pp. 134–142, 2019.

[51] Zhang, Z., Zeng, P., Pan, B., Choo, K.K.R.: Large-universe attribute-based encryption with public traceability for cloud storage. IEEE Internet of Things Journal **7**(10), 10314–10323 (2020)

[52] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Annual international cryptology conference*. Springer, 2001, pp. 213–229.

[53] A. De Caro and V. Iovino, “jpbc: Java pairing based cryptography,” in *Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011*, Kerkyra, Corfu, Greece, June 28 - July 1, 2011, pp. 850–855.

**Teng Li** received the B.S. degree in school of computer science and technology from Xidian University, China in 2013, and Ph. D. degree in school of computer science and technology from Xidian University, China in 2018. He is currently a lecturer at the school of cyber engineering, Xidian University, China. His current research interests include wireless and mobile networks, distributed systems and intelligent terminals with focus on security and privacy issues.

**Jiawei Zhang** received the B.S. and M.S. degrees in School of Telecommunications Engineering from Xidian University, China, in 2007 and 2010, respectively. He is currently pursuing the Ph.D. degree with the School of Computer Science and Technology in Xidian University, China. His current research interests include access control, data security, cloud and edge security, blockchain, cryptography and network security.

**Yanbo Yang** received the B.S. and Ph.D degrees in School of Telecommunications Engineering from Xidian University, China, in 2006 and 2014, respectively. Now He is lecture in Information Engineering School of Inner Mongolia University of science and technology, China. He is currently pursuing the fusion application of UAV/UGV, Blockchain technology, big data and machine learning in Industrial Internet area. Yanbo Yang is the corresponding author.

**Wei Qiao** received the B. S. degree from Xidian University, Xi’an, China in 2021. His research interests include attack detection, networksecurity, cryptography and information security.

**Yangxu Lin** is currently pursuing the master’s degree with School of Cyber Engineering, Xidian University. His current research interests include UAV communication security, wireless communication.