A Dynamic Access Control Scheme with Conditional Anonymity in Socio-Meteorological Observation

Tiantian Miao[1,2]*, Chin-Feng Lai*[3]*, Jian Shen*[4*]*, Baojun Liu*[2]*, Chen Wang*[4]

[1] *Key Laboratory for Meteorological Disaster Prevention and Mitigation of Shandong, China*
[2] *Comprehensive Meteorological Supporting Center, Qingdao Meteorological Bureau, China*
[3] *Department of Engineering Science, National Cheng Kung University, Taiwan*
[4] *School of Information Science and Engineering, Zhejiang Sci-Tech University, China*
mtt_0106@126.com, cinfon@ieee.org, s_shenjian@126.com, qdlbj@163.com, wangchen@zstu.edu.cn

Abstract

Socio-meteorological observation is an essential part of meteorological information construction, where unofficial organizations and individuals (volunteers) are employed to collect meteorological data. Thanks to the participation of social forces, the density and richness of meteorological data are improved significantly, and hence more economical and social benefits are brought. However, problems such as privacy leakage and data islands hamper the sustainable development of socio-meteorological observation. To solve the problems, we propose a dynamic access control scheme with conditional anonymity in socio-meteorological observation. In the proposed scheme, conditional anonymity of volunteers is supported. On the one hand, the real identity of each valid volunteer is private; On the other hand, the real identity of the malicious volunteers will be revealed if they attempt to inject erroneous meteorological data into the system. In addition, a lazy update mechanism is designed, where the fluidity of the volunteers and attribute revocation of the data users are fully considered. Finally, we compare the proposed scheme with similar schemes theoretically and experimentally.

Keywords: Conditional anonymity, Attribute revocation, Access control, Socio-meteorological

1 Introduction

Socio-meteorological observation [1] is a new observation mode, where meteorological observation activities are carried out by individuals or groups outside the meteorological industry. The meteorological data is mainly from 1) meteorological detection equipment built by research institutions, volunteers and enterprises; 2) Meteorological element sensors deployed in smartphones, smart homes, intelligent transportation [2], etc. 3) Statistical analysis of sensitive words about meteorology by search engines. For simplicity, all social forces are denoted as volunteers in this paper. Compared with traditional meteorological observation, socio-meteorological observation has advantages over the space-time density and richness of meteorological data. Therefore, the accuracy of the meteorological data is improved. In addition, socio-meteorological observation makes up for areas not covered by conventional weather station observations.

Meteorological data security is crucial for the interests of the general public. With the development of socio-meteorological observation, more and more people are participating in this observation mode, and the amount of meteorological data is increased exponentially. To manage meteorological data flexibly, volunteers would like to sharing these data through the cloud. However, the cloud is seemed to be honest-but-curious [3]. The potential security issues mentioned above may bring significant losses at any time [4]. Ciphertext-based encryption (ABE) technologies [5] have been the natural choice to ensure the data access security, since they are flexible and fine-grained.

Besides access security, the authenticity of meteorological data is also important [6-7]. If the data set is mixed with abnormal data, the results of the disaster warning may seriously deviate from the facts. Therefore, it is necessary to establish linkages between meteorological data and data acquisition devices. If the data is right, no extra operations are required. However, once abnormal data is detected, the system can quickly locate the specific device collecting the data. Then, the device is repaired or replaced. However, volunteers do not want their private information to be exposed to the public. Hence, how to simultaneously meet the requirements of anonymity and traceability [8] has been a challenge.

Dynamic operations of volunteers and data consumers should also be considered. In socio-meteorological observation, a volunteer will be removed if his devices are failed beyond repair. Meanwhile, there are also new volunteers joining the observation system [9]. From the perspective of data consumers, their attributes are not constant. As a countermeasure, lazy update mechanism for efficient key update [10] is necessary.

1.1 Main Contributions

To address the challenges mentioned above, we proposed a dynamic access control scheme with conditional anonymity in socio-meteorological observation. Especially, our main contributions are summarized as follows.

---

*Corresponding Author: Jian Shen; E-mail: s_shenjian@126.com

DOI: 10.53106/160792642023092405001

1) *A General Framework for Access Control in Socio-Meteorological Observation Is Constructed.* In the framework, each data consumer can obtain some privileges according to their attributes. In other words, a data consumer cannot access target data if he does not have the specified attributes. As a result, accurate configuration of meteorological data is realized.

2) Conditional Anonymity for Volunteers Is Supported. If the observation system runs normally, private information such as identity is private. If meteorological data is in doubt, the data is traceable to the specific device collecting the data.

3) The Mechanism of Lazy Update Is Designed. In real life scenarios, volunteers may join or exit the observation system, the attribute set of data consumers can also be reconstructed. To ensure the forward and backward secrecy, we introduce the lazy update mechanism, where both dynamic operations of volunteers and the attribute revocation are ensured efficiently.

1.2 Related Works

Access control is one of the most important methods to guarantee the security of the outsourced data. Due to their excellent performance in flexibility and fine granularity, access control schemes have attracted much attention [10-14]. In 2005, Sahai *et al.* [15] first put forward the concept of attribute-based encryption (ABE). In 2006, Goyal *et al.* [16] found the data in Sahai *et al.*'s scheme only can be shared at a coarse-grained level. Then, they developed a new cryptosystem named Key-Policy Attribute-Based Encryption (KP-ABE). However, the KP-ABE proposed by Goyal *et al.* performs poorly in scalability and accountability. Motivated by this, Yu *et al.* [17] designed a scalable and fine-grained data access control scheme based on re-encryption technologies. In 2015, Wang *et al.* [18] pointed out the inefficiency of Yu *et al.*'s method, and proposed an adaptive secure outsourcing CP-ABE scheme. Subsequently, Wang *et al.* [19] improved the above traditional ABE schemes by designing a file hierarchy attribute-based encryption scheme. To further ensure the privacy of data consumers, Belguith *et al.* [20] designed a new ABE, which hides policies for cloud-assisted IOT. Recently, Deng *et al.* [21] designed a new attribute-based data storage scheme, where the dynamic operations of data consumers are considered.

From the above analysis, we can see that the existing schemes mainly focus on protecting data content, while ignoring the negative impact brought by data source distortion and the dynamic operations of users. Therefore, we intend to design a new access control scheme, which simultaneously meets the needs of anonymity, traceability and scalability.

2 Preliminaries

2.1 Bilinear Pairing

$\mathcal{G}$ and $\mathcal{G}_T$ are cyclic multiplicative groups, g is a generator of $\mathcal{G}$, the large prime q is the order of the above two groups. $\hat{e}: \mathcal{G}\times\mathcal{G} \rightarrow \mathcal{G}_T$ is a bilinear map [22], if:

(1) Bilinearity: For any $g, h \in \mathcal{G}$ and any $a, b \in \mathcal{Z}_q^*$, we have $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$.

(2) Non-degeneracy: For any $g, h \in \mathcal{G}$, we have $\hat{e}(g, h) \neq 1$.

(3) Computability: For any $g, h \in \mathcal{G}$, $\hat{e}(g, h)$ can be calculated.

2.2 Linear Secret Sharing Schemes (LSSS) [23]

We set U as the attribute universe. An LSSS includes $(\mathcal{M}, \rho)$, where $\mathcal{M}$ denotes a $l \times n$ matrix over $\mathcal{Z}_q^*$, and ρ maps a row of $\mathcal{M}$ into an attribute in U. An LSSS is comprised of the following two algorithms:

(1) Share $((\mathcal{M}, \rho), s)$: Let $\boldsymbol{v} = (s, y_2, y_3, ..., y_n)$ be a random vector, where $s, y_2, y_3, ..., y_n \in \mathcal{Z}_q^*$. Then, compute $\lambda_x = \mathcal{M}_x \cdot \boldsymbol{v}$ as a secret share of s.

(2) Reconstruction $((\lambda_1, \lambda_2, ..., \lambda_l, (\mathcal{M}, \rho))$: For any authorized set S, there exists coefficients $\{w_i\}_{i \in S}$, such that $\sum_{i \in S} \omega_i \mathcal{M}_i = (1, 0, ..., 0)$. Finally, we have $\sum_{i \in S} \omega_i \lambda_i = s$.

(3) We say that S satisfies $(\mathcal{M}, \rho)$, if there exits coefficients $\{w_i\}_{i \in S}$ such that $\sum_{i \in S} \omega_i \mathcal{M}_i = (1, 0, ..., 0)$.

3 Problem Statement

3.1 System Model

The system model of the access control scheme includes five participants as shown in Figure 1:

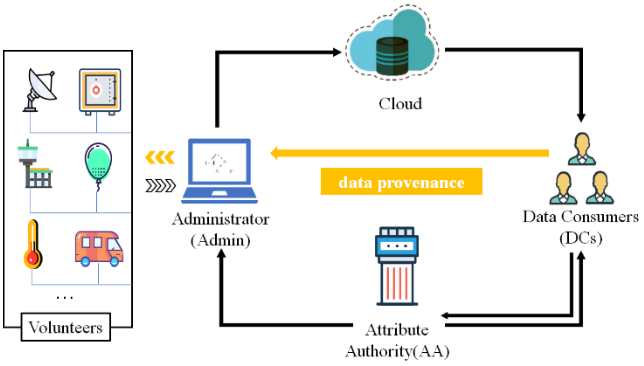

Figure 1. The system model

Administrator (Admin) is the sponsor of a socio-meteorological observation project. It is responsible for data processing, access policies construction, registration and data provenance.

Volunteers are data collectors. They are mainly in charge of transferring the collected data to Admin.

Attribute Authority (AA) is a fully trusted party. It is primarily responsible for managing attributes and generating decryption keys.

Cloud has abundant computing and storage resources. It will not change the meteorological data, but attempts to recover the content of the meteorological data.

Data Consumers (DCs): Each DC has a series of attributes. If they want to access the meteorological data, they send their attributes to the AA and acquire their decryption key.

3.2 Design Goals

In this paper, we mainly consider the following five requirements.

1) Privacy-saving means that the private information of volunteers, such as real identity, is unknown to the public. Motivated by this, pseudonyms rather than their real identities are employed.

2) Traceability refers the conditional anonymity of volunteers. On the one hand, the real identity of volunteers is private; On the other hand, once abnormal meteorological data is detected, the volunteer owing the data is traced.

3) Attribute revocation allows DCs to change their attributes and AA to update the decryption key of DCs associated with the revoked attributes.

4) Forward and backward secrecy: Forward secrecy means that DCs cannot access the previous data with new attributes; backward secrecy refers to that DCs cannot access the latter data with old attributes.

4 The Proposed Scheme

For convenience, we take the temperature data *temp* as an example to introduce our scheme.

4.1 Initialization

The *Initialization* is composed of two phases:

1) *SetUp*: Let $\mathcal{G}$ and $\mathcal{G}_T$ be two cyclic groups with the same order q. g is a generator of $\mathcal{G}$. $\hat{e}: \mathcal{G}\times\mathcal{G} \rightarrow \mathcal{G}_T$ is a bilinear map. Let U be an attribute universe, and $|U|$ be the size of U. Admin chooses hash functions $\mathcal{H}_1$: $\{0, 1\}^* \rightarrow \mathcal{Z}_q^*$ and $\mathcal{H}_2$: $\mathcal{G} \rightarrow \mathcal{Z}_q^*$, random numbers a, $\alpha \in \mathcal{Z}_q^*$, and elements $h_1, h_2, ..., h_{|U|} \in \mathcal{G}$. Then, Admin computes the public key PK and the master secret key MSK as Eq.(1) and Eq.(2).

$$PK = \left\{U, g, g^a, \hat{e}(g,g)^{\alpha}, h_1, ..., h_{|U|}, \mathcal{H}_1, \mathcal{H}_2\right\}. \tag{1}$$

$$MSK = g^{\alpha}. \tag{2}$$

2) *Registration*: This algorithm is divided into two steps:

The first step is to generate a key pair $\{PK_A, SK_A\}$ for Admin and key pairs $\{PK_{V_i}, SK_{V_i}\}$ for volunteers. For the Admin, he randomly selects an integer $s_A \in \mathcal{Z}_q^*$ as his secret key SK_A, and computes $PK_A = g^{sA}$ as his public key. Similar with the Admin, the key pair of each volunteer is set as $PK_{V_i} = g^{s_{V_i}}$ and $SK_{V_i} = s_{V_i}$, where $s_{V_i} \in \mathcal{Z}_q^*$.

The second step is to distribute a pseudonym for each volunteer. Each volunteer sends his real identity ID_i to Admin through a secure channel. Admin randomly selects an integer $a_i \in \mathcal{Z}_q^*$, a string arr_i, and calculates $A_i = a_i + \mathcal{H}_1(ID_i\|arr_i)$, $B_i = g^{a_i}$, $pseud_i = g^{\mathcal{H}_1(ID_i\|arr_i)}$. After receiving the tuple $\{A_i, B_i, pseud_i\}$, the volunteer verifies Eq.(3).

$$g^{A_i} ?= B_i \cdot pseud_i. \tag{3}$$

If Eq.(3) holds, the volunteer accepts $pseud_i$ as his pseudonym. Finally, Admin appends the tuple $\{pseud_i, ID_i$, credibility$\}$ to Volunteer Record Table (VRT) as shown in Table 1. In VRT, credibility is presented as $\text{cred}_i = err_i / total_i$, which means that volunteer V_i sends $total_i$ data packets to Admin, but err_i data packets is inaccurate. If a volunteer exits the system, his credibility value is set to be −1.

Table 1. The volunteer record table

Pseudonym	Real identity	Credibility
$pseud_1 = g^{\mathcal{H}_1(ID_1\|arr_1)}$	ID_1	80%
$pseud_2 = g^{\mathcal{H}_1(ID_2\|arr_2)}$	ID_2	-1
…	…	…

4.2 Encryption

In this algorithm, volunteers collect local temperatures, and transmit these raw data *rtemp* to Admin. Admin standardizes these data from *rtemp* to *TEMP*, and shares the ciphertext of *TEMP* through the Cloud.

Table 2. The data transfer format (bytes)

<table>
<tr><td>Latitude (6)</td><td>Longitude (7)</td><td>Altitude (5)</td><td>Time (14)</td></tr>
<tr><td colspan="4">The number of observation elements (3)</td></tr>
<tr><td colspan="2">Temperature (3)</td><td colspan="2">The value of temperature (4)</td></tr>
<tr><td colspan="2">The second element E_2 (…)</td><td colspan="2">The value of E_2 (…)</td></tr>
<tr><td colspan="2">…</td><td colspan="2">…</td></tr>
</table>

For each volunteer, he collects the local temperature $rtemp_i$. Note that the format of $rtemp_i$ is shown as Table 2. Then, the volunteer computes $\text{len}_i = \mathcal{H}_2(ID_i)$, randomly selects two strings $str_{i,1}$ and $str_{i,2}$. Note that the length of $str_{i,1}$ is len_i, while the $str_{i,2}$ is with random length. The volunteer sets CT_{rtemp_i} as Eq.(4).

$$CT_{rtemp_i} = str_{i,1} \| rtemp_i \| str_i. \tag{4}$$

Finally, V_i computes $SV_i = pseud_i \cdot PK_A^{SV_i}$, and sends $\{SV_i, CT_{rtemp_i}\}$ to the Admin.

Then, Admin recovers the temperature $temp_i = CT_{rtemp_i}[len_i + 38, len_i + 42]$, sets $total_i = total_i + 1$ and constructs a function $\Theta: temp_i \rightarrow SV_i$. After receiving all $temp_i$ in monitoring regional, Admin aggregates these data as $TEMP = \{temp_1, temp_2, ...\}$, and denotes $SV = \{SV_1, SV_2, ...\}$. Next, Admin selects a session key φ and encrypts $TEMP$ as Eq.(5),

$$CT_{TEMP} = \mathcal{E}nc_{\varphi}(TEMP.) . \tag{5}$$

where $\mathcal{E}nc$ is a symmetric encryption algorithm. To ensure the secure sharing of the $TEMP$, the session key φ is also encrypted based on ABE. Concretely, Admin constructs an access structure $\mathcal{T} = (\mathcal{M}_{l\times n}, \rho)$, where ρ correlates each row of the matrix $\mathcal{M}$ to an attribute. Next, Admin selects $n-1$ random elements $y_2, y_3, ..., y_n \in \mathcal{Z}_q^*$ and forms the vector $\boldsymbol{v} = (s, y_2, y_3, ..., y_n)$. For each attribute $\forall\, i \in [1, l]$, Admin calculates $\lambda_i = \mathcal{M}_i \cdot \boldsymbol{v}$, and sets $CT_{\varphi} = \{C, C', \{C_i\}_{i\in[1,l]}$, where

$$C=\varphi\cdot\hat{e}(g,g)^{\alpha s};C'=g^{s};C_i=g^{a\lambda_i}h_i^{-s\cdot v_{i,ver}}. \tag{6}$$

Finally, the tuple $\{CT_{TEMP}, CT_{\varphi}, SV\}$ is uploaded to the cloud.

4.3 Key Generation

To get the decryption key, DCs send his attributes $S\subseteq 2^U$ to AA. Then, AA generates the decryption key DK for DCs: Firstly, AA randomly chooses a number $t\in\mathcal{Z}_q^*$. For each attribute $A\in S$, AA randomly selects $v_{i,ver}\in\mathcal{Z}_q^*$, where ver denotes the number of times the attributes has been updated. For example, $v_{2,7}$ represents the attribute A_2 has been updated 7 times. Finally, AA computes Eq.(7), and sets the decryption key of the DC as $DK=\{K, K', \{K_i\}_{i\in S}$.

Algorithm 1. Add a new volunteer to VRT

```
Input: $pseud_+$, $ID_+$ and the VRT
Output: the update VRT
Let $Row\_Number$ be the valid rows of the VRT
for $index = 0$ to $Row Number - 1$ do
  if $VRT[index][2] == -1$ then
    break
  end if
end for
if $index \le Row\_Number - 1$ then
  $VRT[index][0] = pseud_+$
  $VRT[index][1] = ID_+$
  $VRT[index][2] = 1$
else
  $VRT[Row\_Number][0] = pseud_+$
  $VRT[Row\_Number][1] = ID_+$
  $VRT[Row\_Number][2] = 1$
end if
```

$$K=g^{\alpha}g^{at};K'=g^{t};\left\{K_i=h_i^{tv_{i,ver}}\right\}_{i\in s}. \tag{7}$$

4.4 Decryption

DCs first check whether there are attributes A satisfying the access structure $\mathcal{T}$. If A does not exist, then the DC cannot access the target data; Otherwise, the DC executes the following steps:

The first step is to obtain the session key φ. Given the properties of the LSSS, the DC can easily select a series of constants $\{w_i\in\mathcal{Z}_q^*\ _{i\in A}$ such that $\sum_{i\in S}\omega_i\mathcal{M}_i=(1,0,...,0)$. The DC computes Eq.(8).

$$\frac{\hat{e}\left(C',K\right)}{\hat{e}\left(\prod_{i\in A}C_i^{\omega_i},K\right)e\left(C',\prod_{i\in A}K_i^{\omega_i}\right)}=\hat{e}\left(g,g\right)^{\alpha s}. \tag{8}$$

Subsequently, the session key is computed as $\varphi=\frac{C}{\hat{e}\left(g,g\right)^{\alpha s}}$.

The second step is to decrypt the target data $TMEP$. Based on φ and $\mathcal{E}nc$, the DC can finally derive the temperature data $TMEP$.

4.5 Data Provenance

In this algorithm, if DCs have doubts over the data set $TMEP$, they report it to Admin. According to the report, Admin decides whether to trace the data.

For example, a station's temperature is −10°C. However, at the same time, the temperature of its surrounding stations is around 20°C. Then, the temperature monitored by the station is deemed as abnormal data. For simplicity, we set the abnormal data as $temp_{\times}\in TEMP$, and denote the volunteer monitoring the data as $V_{\times}$. If $temp_{\times}$ is abnormal, Admin does the following steps: Firstly, Admin calls the function $\Theta:temp_{\times}\rightarrow SV_{\times}$ and recovers the pseudonym of the volunteer $V_{\times}$ by computing $pseud_{\times}=\frac{SV_{\times}}{PK_{V_{\times}}{}^{s_A}}$. Then, the real identity $ID_{\times}$ of the volunteer is revealed by enquiring about the VRT. Finally, Admin sets $err_{\times}=err_{\times}+1$ and updates $pseud_{\times}=\frac{err_{\times}}{total_{\times}}$.

4.6 Lazy Update

Four dynamic operations of volunteers and the DC are analyzed here.

Case 1: If a volunteer V_- wants to exit the socio-meteorological observation system, he delivers $\{pseud\_, exit\}$ to AA. Based on the $pseud_-$, AA traverses the VRT and gets the $index$, where $VRT[index_-][0]==pseud_-$. Finally, the credibility of the volunteer $cred_-=VRT[index_-][2]$ is set to be −1.

Case 2: If a volunteer V_+ wants to join system, he delivers $\{pseud_+, ID_+, join\}$ to AA. Then AA computes $A_+=a_++\mathcal{H}_1(ID_+\|arr_+)$, $B_+=g^{a_+}$ and $pseud_+=g^{\mathcal{H}_1(ID_+\|arr_+)}$, where $a_+\in\mathcal{Z}_q^*$ is a random integer, $attr_+$ is a random string. Subsequently, V_+ verifies if $g^{A_+}?=B_+\cdot pseud_+$ holds. If true, V_+ accepts $pseud_+$ as his pseudonym. Finally, V_+'s information is added to the VRT through Algorithm 1.

Case 3: If a DC wants to add an attribute $attr_+$, he sends the tuple $\{attr_+, add\}$ to AA. Then, AA randomly selects an integer $v_{+,ver+1}$ and calculates $K_+=h_+^{t\,v_{+,ver+1}}$. Finally, the decryption keys of the all DCs holding $attr_+$ are updated as Eq.(9).

$$K=K;K'=K';K_i=\begin{cases}\left\{K_i\right\}_{i\in s\backslash attr_+}\\ \left\{h_i^{t^{v_{i,ver+1}}}\right\}_{i=attr_+}\end{cases}. \tag{9}$$

Case 4: Similar with the Case 3, AA updates the decryption keys of the all DCs holding $attr\_$ as Eq.(10).

$$K=K;K'=K';K_i=\begin{cases}\left\{K_i\right\}_{i\in s\backslash attr-}\\ \left\{h_i^{t^{v_{i,ver+1}}}\right\}_{i=attr-}\end{cases}. \tag{10}$$

where $v_{-,ver+1}$ is an random integer.

5 Evaluation

5.1 Security Analysis

***Theorem* 1: The proposed dynamic access scheme is correct.**

***Proof*:** In our scheme, all volunteers get their pseudonyms from the Admin. Based on the pseudonym, they monitor and transfer the temperature data without disclosing their private information. DCs obtain these data if their attributes satisfy the access structure. Therefore, Theorem 1 relies on the correctness of the *Registration* and the *Decryption*.

Lemma 1. In *Registration*, A volunteer accepts $pseud_i$ as his pseudonym if and only if $g^{A_i} ?= B_i \cdot pseud_i$ holds. The proof of the equation is given as Eq.(11):

$$\begin{aligned} g^{A_i} &= g^{a_i + \mathcal{H}_1(ID_i \| arr_i)} \\ &= g^{a_i} \cdot g^{\mathcal{H}_1(ID_i \| arr_i)} \\ &= B_i \cdot pseud_i. \end{aligned} \tag{11}$$

Therefore, Lemma 1 is proved.

Lemma 2. In *Decryption*, if a DC wants to access the data *TEMP*, he needs acquire the session key φ. Based on φ and $\mathcal{E}nc$, he can further recover the data from CT_{TEMP}. Note that the precondition for recovering the session key φ is the equation $\frac{\hat{e}(C',K)}{\hat{e}\left(\prod_{i\in A} C_i^{\omega_i}, K\right) e(C', \prod_{i\in A} K_i^{\omega_i})} = \hat{e}(g,g)^{\alpha s}$ holds, which is proved as Eq.(12):

$$\begin{aligned} &\frac{\hat{e}(C',K)}{\hat{e}\left(\prod_{i\in A} C_i^{\omega_i}, K\right) e(C', \prod_{i\in A} K_i^{\omega_i})} \\ &= \frac{\hat{e}(g^s, g^\alpha g^{at})}{\hat{e}(\prod_{i\in A} g^{a\lambda_i} h_i^{-s\cdot v_{i,ver}\omega_i}, g^t) e(g^s, \prod_{i\in A} (h_i^t)^{v_{i,ver}\cdot\omega_i})} \\ &= \frac{\hat{e}(g,g)^{\alpha s} \cdot e(g,g)^{ast}}{\hat{e}(g^{\Sigma_{i\in A}\lambda_i\omega_i}, g)^{at}} \\ &= \hat{e}(g,g)^{\alpha s}. \end{aligned} \tag{12}$$

Then, the DC further computes $\frac{C}{\hat{e}(g,g)^{\alpha s}} = \frac{\varphi \cdot \hat{e}(g,g)^{\alpha s}}{e(g,g)^{\alpha s}} = \varphi$. Finally, the DC easily derives the temperature data *TMEP*. Therefore, Lemma 2 is proved, and Theorem 1 is proved.

***Theorem* 2. Privacy-saving and traceability refer to that no one except for Admin can get the real identity of the volunteers.**

Proof. On the one hand, to private the privacy of volunteers, pseudonym $pseud_i = g^{\mathcal{H}_1(ID_i\|arr_i)}$ rather than their real identity ID_i are employed to communicate with others. Note that the relationship between $pseud_i$ and ID_i is recorded in VRT, which is held by Admin. In other words, any participant except for the Admin cannot get the real identity of the volunteers. Hence, the privacy of volunteers is saved.

On the other hand, once abnormal data $temp_i$ is detected, the tuple $\{temp_i, SV_i\}$ will be reported to the Admin. Furthermore, Admin recovers the pseudonym by Eq.(13).

$$\frac{SV_i}{PK_{V_i}^{\ s_A}} = \frac{pseud_i \cdot PK_A^{\ s_{V_i}}}{g^{s_{V_i} s_A}} = pseud_i. \tag{13}$$

Then, Admin queries the VRT and get ***index***, where ***VRT***[***index***][**0**] = $pseud_i$. Finally, the real identity of the volunteer is derived as ID_i = ***VRT***[***index***][**1**]. Therefore, the traceability of the temperature data is supported. Hence, Theorem 2 is further proved.

***Theorem* 3. The forward secrecy and backward secrecy of the temperature data are ensured.**

Proof. We assume that DC_+ adds a new attribute $attr_+$ in time t_f. $TEMP_+$ denotes all the data sets that relate to the $attr_+$ and generate before t_f. Forward secrecy refers to DC_+ can not access $TEMP_+$ with the new attribute $attr_+$.

From the analysis of Case 3, AA computes and delivers $K_+ = h_+^{t\, v_{+,ver+1}}$ to all DCs involving the $attr_+$. Hence, part of the decryption key is updated as $K_i = \left\{\{K_i\}_{i\in S\setminus attr_+}; \{h_i^{t v_{i,ver+1}}\}_{i=attr_+}\right\}$. Then, DC_+ obtains session key by calculating Eq.(14).

$$\begin{aligned} &\frac{\hat{e}(C',K)}{\hat{e}\left(\prod_{i\in A} C_i^{\omega_i}, K\right) e(C', K_+^{\ \omega_+} \prod_{i\in A\setminus attr_+} K_i^{\omega_i})} \\ &= \frac{\hat{e}(g,g)^{\alpha s}}{\hat{e}\left(h_+^{v_{+,ver}\omega_+}, g^t\right)^{-st} \hat{e}\left(g, h_+^{v_{+,ver+1}\omega_+}\right)^{st}} \\ &\neq \hat{e}(g,g)^{\alpha s}. \end{aligned} \tag{14}$$

Furthermore, the session key φ and $TEMP_+$ can not be accessed by the DC. Therefore, the forward secrecy is ensured.

Contrary to forward secrecy, backward secrecy points that DC_- can not access $TEMP_-$ with the old attribute $attr_-$. From the above analysis, we can easily conclude that

$$\begin{aligned} &\frac{\hat{e}(C',K)}{\hat{e}\left(\prod_{i\in A} C_i^{\omega_i}, K\right) e(C', K_-^{\ \omega_-} \prod_{i\in A\setminus attr_-} K_i^{\omega_i})} \\ &\neq \hat{e}(g,g)^{\alpha s}. \end{aligned} \tag{15}$$

Hence, the session key φ and $TEMP_-$ can not be recovered. Then, the backward secrecy is ensured. Hitherto, Theorem 3 is proved.

5.2 Performance Analysis

(1) *Theoretical Analysis*: Here, we first compare our scheme with Liu's [24] scheme, Jung's [25] scheme and Deng's scheme [21] in terms of some important functions. The results are given as Table 3. From Table 3, we can

conclude that: 1) Access security of the outsourced data is improved in the above four schemes. 2) Neither privacy-saving nor traceability is realized in Liu's scheme and Deng's scheme; Jung's scheme protects the privacy information of volunteers while ignoring the requirement of data provenance; Compared with the related schemes, only the proposed scheme meets the requirements of anonymity and traceability simultaneously. 3) Only Deng's scheme and the proposed scheme support attribute revocation and ensure the forward and backward secrecy. According to the above analysis, Deng's scheme and the proposed scheme have a better performance in the above six functions.

In socio-meteorological observation systems, computational overhead is an important evaluation factor. Therefore, Deng's scheme is chosen for further comparerison in Table 4. For discussion convenience, we let l be the number of rows in an access matrix, $|A|$ the number of a DC's attributes. Additive operation and connection operation are ignored for their negligible cost. Table 4 shows that the proposed scheme requires less computational overhead than that of Deng in *Encryption*, *Key Generation*, *Decryption* and *Attribute Revocation*. Moreover, DCs are only allowed to revoke their attributes no more than Max times in Deng's scheme, which is no restriction in our scheme. In conclusion, the proposed scheme realizes more functions with lower overhead.

Table 3. Comparison of access control schemes in terms of some important functions

Schemes	Access security	Privacy saving	Traceability	Attribute revocation	Forward secrecy	Backward secrecy
Liu's Scheme	√	×	×	×	√	×
Jung's scheme	√	√	×	×	×	×
Deng's scheme	√	×	×	√	√	√
The proposed Scheme	√	√	√	√	√	√

Table 4. Comparison of access control schemes in terms of computational overhead

Schemes	Encryption	Key generation	Decryption	Attribute revocation
Deng's scheme	$P + (Max + 3l + 3)\,E$ $+ (Max/\,2)\,M$	$(Max + \|A\| + 4)\,E$ $+ (Max/\,2)\,M$	$(2\|A\| + 2)\,P + (2\|A\| - 1)\,E$ $+ (\|A\| + 2)\,M$	$4\,E + 2M$
The proposed Scheme	$P + (2l + 2)\,E$ $+ (3l + 2)\,M$	$(\|A\| + 3)\,E$ $+ (\|A\| + 1)\,M$	$3P + 2\|A\|\,E$ $+ (2\|A\| - 1)\,M$	$3\,E$

* P: logarithm operation; E: the exponent arithmetic; M: the multiplication operation.

2) *Experimental Analysis*: We conduct the simulation on a mobile device. Note that each operation is executed 100 times and the average time cost is chosen, which reduces the occasionality of experimental results. The results are shown as Figure 2 to Figure 5.

In Figure 2 and Figure 3, we compare the time cost of the *Encryption* and *Key Generation*. For ease of description, we set $Max = 1000$. From Figure 2, we know that if $l \leq 1000$, the time cost is much more than that of the proposed scheme. Same as Figure 2, the proposed scheme needs less time cost in *Key Generation*. In reality, the access policy of a data and the attribute set of a DC are not so complex. Hence, the proposed scheme is more practical in *Encryption* and *Key Generation*. The time cost for *Decryption* is compared in Figure 4. From the figure, we know that the time cost of the two schemes increases with the increasing of the size of DC's attribute set. However, the time cost of Deng's scheme increases more sharply. Finally, the time cost for *Attribute Revocation* is compared in Figure 5. From Figure 5, we can see that both the two schemes' time cost is not changed with the increasing of number of attributes. However, the proposed scheme requires less time cost if a DC wants to revoke an attribute. In summary, the proposed scheme has a better performance in computational overhead.

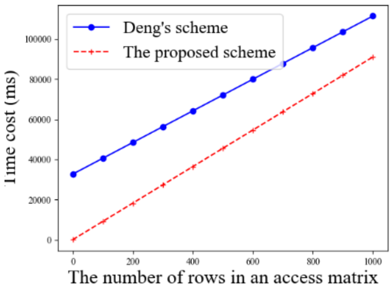

Figure 2. Time cost for encryption

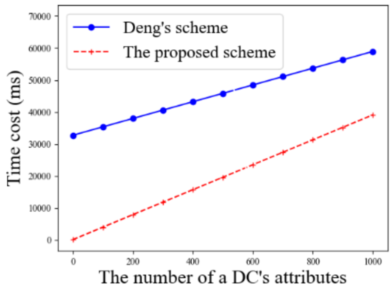

Figure 3. Time cost for key generation

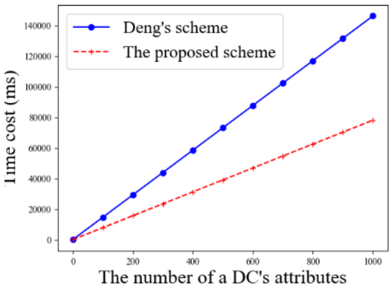

Figure 4. Time cost for decryption

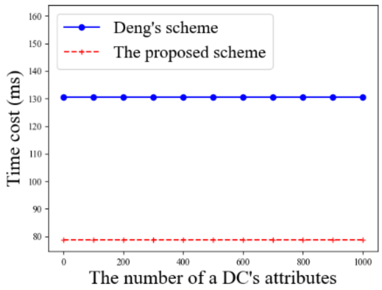

Figure 5. Time cost for revoking an attribute

6 Conclusion

To accelerate the development of socialized meteorological observation, we propose a dynamic access control scheme with conditional anonymity in socio-meteorological observation. More specifically, a general framework for secure meteorological data access control is designed, which prevents meteorological data from being misused. Subsequently, conditional anonymity for volunteers is realized. For one thing, the private information of volunteers is protected. For another, the traceability of abnormal meteorological data is supported. In addition, a lazy update mechanism is presented, where dynamic operations of volunteers and attribute revocation are allowed. Finally, theoretical and experimental analyses prove the proposed scheme realized more functions with less computational overhead.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grants No. 61922045, No. U21A20465, No. 62172292, No. 61877034, the Science and Technology Research Project of Shandong Meteorological Bureau under Grants No. 2021SDQN19.

References

[1] A. M. Droste, J. J. Pape, A. Overeem, H. Leijnse, G. J. Steeneveld, A. J. Van Delden, R. Uijlenhoet, Crowdsourcing urban air temperatures through smartphone battery temperatures in São Paulo, Brazil, *Journal of Atmospheric and Oceanic Technology*, Vol. 34, No. 9, pp. 1853-1866, September, 2017.

[2] S. A. Khowaja, P. Khuwaja, K. Dev, I. H. Lee, W. U. Khan, W. Wang, N. M. F. Qureshi, M. Magarini, A Secure Data Sharing Scheme in Community Segmented Vehicular Social Networks for 6G, *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 1, pp. 890-899, January, 2023.

[3] J. Shen, T. Zhou, X. Chen, J. Li, W. Susilo, Anonymous and traceable group data sharing in cloud computing, *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 4, pp. 912-925, April, 2018.

[4] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, An Adaptive Physical Layer Key Extraction Scheme for Smart Homes, *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 499-506.

[5] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, *2007 IEEE Symposium on Security and Privacy—SP'07*, Berkeley, CA, USA, 2007, pp. 321-334.

[6] W. Wang, Z. Han, M. Alazab, T. R. Gadekallu, X. Zhou, C. Su, Ultra Super Fast Authentication Protocol for Electric Vehicle Charging Using Extended Chaotic Maps, *IEEE Transactions on Industry Applications*, Vol. 58, No. 5, pp. 5616-5623, September-October, 2022.

[7] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N. M. F. Qureshi, In the Digital Age of 5G Networks: Seamless Privacy-Preserving Authentication for Cognitive-Inspired Internet of Medical Things, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 12, pp. 8916-8923, December, 2022.

[8] R. Li, J. Shen, S. Tan, K. C. Li, A secure and efficient conditional anonymous scheme for permissionless blockchains, *Journal of Internet Technology*, Vol. 22, No. 6, pp. 1215-1227, November, 2021

[9] J. Shen, T. Miao, J.-F. Lai, X. Chen, J. Li, S. Yu, Ims: An identity-based many-to-many subscription scheme with efficient key management for wireless broadcast systems, *IEEE Transactions on Services Computing*,

Vol. 15, No. 3, pp. 1707-1719, May-June, 2022.

[10] H. Zhao, Y. Zhang, X. Huang, Y. Xiang, C. Su, A Physical-Layer Key Generation Approach Based on Received Signal Strength in Smart Homes, *IEEE Internet of Things Journal*, Vol. 9, No. 7, pp. 4917-4927, April, 2022.

[11] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with non-monotonic access structures, *Proceedings of the 14th ACM Conference on Computer and Communications Security—CCS'07*, Alexandria, Virginia, USA, 2007, pp. 195-203.

[12] Q. Zhao, Y. Zhang, G. Zhang, H. Wang, Ciphertext-policy attribute based encryption supporting any monotone access structures without escrow, *Chinese Journal of Electronics*, Vol. 26, No. 3, pp. 640-646, May, 2017.

[13] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, X. Huang, Hierarchical and shared access control, *IEEE Transactions on Information Forensics & Security*, Vol. 11, No. 4, pp. 850-865, April, 2016.

[14] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei, P. Hong, An attribute-based controlled collaborative access control scheme for public cloud storage, *IEEE Transactions on Information Forensics & Security*, Vol. 14, No. 11, pp. 2927-2942, November, 2019.

[15] A. Sahai, B. Waters, Fuzzy identity-based encryption, *International Conference on the Theory & Applications of Cryptographic Techniques*, Aarhus, Denmark, 2005, pp. 457-473.

[16] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, *Proceedings of the 13th ACM conference on Computer and Communications Security*, Alexandria, VA, USA, 2006, pp. 89-98.

[17] S. Yu, C. Wang, K. Ren, W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, *2010 Proceedings IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1-9.

[18] H. Wang, Z. Zheng, L. Wu, Y. Wang, Adaptively secure outsourcing ciphertext-policy attribute-based encryption, *Journal of Computer Research and Development*, Vol. 52, No. 10, pp. 2270-2280, October, 2015.

[19] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, W. Xie, An efficient file hierarchy attribute-based encryption scheme in cloud computing, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 6, pp. 1265-1277, June, 2016.

[20] S. Belguith, N. Kaaniche, G. Russello, PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, San Francisco, CA, USA, 2018, pp. 924-927.

[21] H. Deng, Z. Qin, Q. Wu, Z. Guan, H. Yin, Revocable attribute-based data storage in mobile clouds, *IEEE Transactions on Services Computing*, Vol. 15, No. 2, pp. 1130-1142, March-April, 2022.

[22] D. Boneh, M. K. Franklin, Identity-based encryption from the weil pairing, *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology—CRYPTO'01*, Santa Barbara, California, USA, 2001, pp. 213-229.

[23] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in Public Key Cryptography, *Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography*, Taormina, Italy, 2011, pp. 53-70.

[24] Z. Liu, H. Liu, Y. Huo, Data access control protocol for the cloud computing based on ciphertext-policy attribute based encryption (cp-abe), *Netinfo Security*, Vol. 14, No. 7, pp. 57–60, July, 2014.

[25] T. Jung, X. -Y. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 1, pp. 190-199, January, 2015.

Biographies

Tiantian Miao received the M.E. degree in Nanjing University of Information Science and Technology, Nanjing, China, in 2021. She is an Assistant Engineer in Qingdao Meteorological Bureau. Her current research interests are data access control and socio-meteorological observation.

Chin-Feng Lai received the Ph.D. degree in engineering science from National Cheng Kung University, Tainan. Since 2016, he has been an Associate Professor of National Cheng Kung University, Tainan. His research focuses on Internet of Things, e-healthcare, embedded systems, etc.

Jian Shen received the Ph.D. degrees in computer science from Chosun University, South Korea. He is a Professor with the Zhejiang Sci-Tech University, China. His research interests include public cryptography, data auditing and sharing, and information security systems.

Baojun Liu graduated from Chengdu University of Information Technology, Chengdu, China. He is a Senior Engineer in Qingdao Meteorological Bureau. His research interests include equipment support, CINRADSB, and dual linear polarization radar.

Chen Wang received the Ph.D. degree at Nanjing University of Information Science and Technology, Nanjing, China. He is an Associate Professor with the Zhejiang Sci-Tech University, China. His research interests include security in edge-cloud systems and secure aggregation.