Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.055243

ARTICLE

A Verifiable Trust-Based CP-ABE Access Control Scheme for Cloud-Assisted Renewable Energy Systems

Jiyu Zhang[1,*], Kehe Wu[1], Ruomeng Yan[1], Zheng Tian[2], Yizhen Sun[2], Yuxi Wu[2] and Yaogong Guo[3]

[1]Department of Control and Computer Engineering, North China Electric Power University, Beijing, 102206, China

[2]State Grid Information & Communication Company of Hunan Electric Power Corporation, Changsha, 410118, China

[3]State Grid Hunan Electric Power Corporation Chenzhou Power Supply Branch, Chenzhou, 423000, China

*Corresponding Author: Jiyu Zhang. Email: jy_zhang@ncepu.edu.cn

Received: 21 June 2024 Accepted: 28 October 2024 Published: 03 January 2025

ABSTRACT

Renewable Energy Systems (RES) provide a sustainable solution to climate warming and environmental pollution by enhancing stability and reliability through status acquisition and analysis on cloud platforms and intelligent processing on edge servers (ES). However, securely distributing encrypted data stored in the cloud to terminals that meet decryption requirements has become a prominent research topic. Additionally, managing attributes, including addition, deletion, and modification, is a crucial issue in the access control scheme for RES. To address these security concerns, a trust-based ciphertext-policy attribute-based encryption (CP-ABE) device access control scheme is proposed for RES (TB-CP-ABE). This scheme effectively manages the distribution and control of encrypted data on the cloud through robust attribute key management. By introducing trust management mechanisms and outsourced decryption technology, the ES system can effectively assess and manage the trustworthiness of terminal devices, ensuring that only trusted devices can participate in data exchange and access sensitive information. Besides, the ES system dynamically evaluates trust scores to set decryption trust thresholds, thereby regulating device data access permissions and enhancing the system's security. To validate the security of the proposed TB-CP-ABE against chosen plaintext attacks, a comprehensive formal security analysis is conducted using the widely accepted random oracle model under the decisional q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption. Finally, comparative analysis with other schemes demonstrates that the TB-CP-ABE scheme cuts energy/communication costs by 43%, and scales well with rising terminals, maintaining average latency below 50 ms, ensuring real-time service feasibility. The proposed scheme not only provides new insights for the secure management of RES but also lays a foundation for future secure energy solutions.

KEYWORDS

Access control; renewable energy systems (RES); ciphertext-policy attribute-based encryption (CP-ABE); security

1 Introduction

Under the pressure of global warming and fossil fuel depletion, the exploration and utilization of renewable energy systems (RES) [1] have emerged as a prominent global hot topic. With the empowerment of Internet of Things (IoT) technology, RES has effectively monitored various power equipment statuses and precise fault localization. Simultaneously, supported by cloud computing technology, they have efficiently handled the storage, in-depth analysis, and management of vast datasets. Post-analysis by the cloud platform, the acquired data serves internal enterprise users or devices, and serves external government and relevant departments, facilitating further processing, analysis, and application.

However, the deficiencies in permission management and configuration of cloud platforms for RES render them susceptible to unauthorized access, thereby heightening the risk of data leakage. Therefore, ensuring data integrity and privacy in the cloud environments, while restricting access solely to authorized users, has emerged as a pressing research focus. Traditional Role-Based Access Control (RBAC) [2] schemes struggle to adapt to dynamic user roles, trust management, and implementing fine-grained data control within cloud environments. In contrast, Attribute-Based Access Control (ABAC) [3], leveraging the capability to determine access permissions based on various attributes such as users, resources, and environmental factors, coupled with the flexibility and adaptability of access policies achieved through logical attribute combinations, have emerged as a pivotal research avenue for addressing data access control challenges in cloud environments. This solution not only enhances the precision and diversity of control but also protects the data privacy of the cloud environment for RES.

In cloud environments, flexible access and diverse control strategies necessitate attribute-based encryption (ABE) for effective rights management in data access control. Sahai and Waters [4] initially introduced ABE, which can be classified into two types based on whether the access structure is related to the key or the ciphertext: key-policy ABE (KP-ABE) [5] and ciphertext-policy ABE (CP-ABE) [6]. KP-ABE is ideal for scenarios with limited users requiring high flexibility. At the same time, CP-ABE is more appropriate for scenarios involving a large user base that necessitates high scalability. Given the diverse terminals connected to cloud platforms, especially in resource-constrained environments, researchers have focused on offloading computational burdens to edge servers (ES) and cloud service providers (CSP). Schemes that enable efficient outsourcing of decryption tasks have been proposed to reduce computational overhead and enhance system scalability.

Moreover, attribute revocation capabilities have been studied to adapt access rights based on terminal properties and dynamic policies. Recent advancements have also emphasized fine-grained access control through attribute weighting and multi-authority attribute policies, facilitating more decentralized and secure access control solutions. However, challenges persist in managing complex access structures, multi-dimensional permissions, user revocation, and trust management for further exploration and innovation. Table 1 lists the limitations of the existing schemes. A more detailed analysis will be undertaken in the Related Work section.

Table 1: Related work and main limitations

Schemes	Year	Access structure	Main limitations
Xue et al. [7]	2022	LSSS matrix	Does not provide attribute revocation, trust management, and outsourcing decryption
Zhang et al. [8]	2022	LSSS matrix	Does not provide trust management
Zhao et al. [9]	2021	LSSS matrix	Does not provide attribute revocation, and trust management

(Continued)

Table 1 (continued)

Schemes	Year	Access structure	Main limitations
Xu et al. [10]	2022	LSSS matrix	Does not provide attribute revocation, and trust management High computational costs
Ge et al. [11]	2023	LSSS matrix	Does not provide attribute revocation, and trust management Lack of formal security analysis
Li et al. [12]	2022	LSSS matrix	Does not provide attribute revocation, and trust management
Zhang et al. [13]	2022	AND gate	Does not provide attribute revocation, trust management, and outsourcing decryption Complex access structure management
Tao et al. [14]	2024	Binary tree	Does not provide attribute revocation, and trust management
Xu et al. [15]	2021	LSSS matrix	Does not provide trust management, and outsourcing decryption High computational costs
Xiong et al. [16]	2022	Binary tree	Does not provide trust management High computational costs
Ma et al. [17]	2022	AND gate	Does not provide trust management, and outsourcing decryption Complex access structure management
Liu et al. [18]	2024	Blockchain	IoT devices do not have certificates and certificate management is complex
Feng et al. [19]	2024	Blockchain LSSS matrix	Does not provide attribute revocation
Alqbaishi et al. [20]	2024	Blockchain	Does not provide attribute revocation High costs of trust evaluation
Wei et al. [21]	2024	Blockchain	Data sharing between edge devices is not applicable for users accessing IoT devices

Considering the limitations of current research and the unique security characteristics of RES, the designed CP-ABE scheme must continue the existing solution and be able to outsource the decryption of ES. Furthermore, as the attributes assigned to RES devices fluctuate with factors such as working hours, geographical location, and operational requirements, the scheme must support attribute revocation to delete the expired or inapplicable attribute key and other information from the attribute authority. Finally, RES devices lack comprehensive trust management during data interaction with the cloud platform, and their trustworthiness cannot be adequately assessed solely through static attributes. As ES enacts access control strategies for RES devices, the proposed scheme must empower ES with trust management capabilities, which have not been proposed in current schemes, which would enable ES to assess device trustworthiness based on device properties, and successful decryption numbers, and subsequently regulate data access accordingly.

Given the three aforementioned security properties, the contributions of this paper are fourfold:

1) The proposed trust-based ciphertext-policy attribute-based encryption scheme for RES (TB-CP-ABE) achieves the secure communication of RES devices to the encrypted data on the cloud. The use of one-way cryptographic hash functions and bilinear pairing renders TB-CP-ABE a secure access control scheme.

2) The proposed TB-CP-ABE scheme incorporates an attribute revocation algorithm to revoke expired device attributes. The updated attribute keys are issued from AA to the CSP, ES, and data owner (DO). Furthermore, a trust management mechanism allows the DO to specify the minimum trust level required for accessing data. The ES regulates device data access by decrypting the trust threshold, which enhances the scheme's security.

3) The widely accepted formal security analysis based on the q-Bilinear Diffie-Hellman Exponent assumption (q-BDHE) validates the proposed scheme's performance against chosen plaintext attack (CPA) security.

4) Finally, a comprehensive comparative study was conducted to evaluate the proposed TB-CP-ABE, focusing on communication and computation costs. The analysis results reveal that the proposed scheme achieves a superior tradeoff between communication and computation costs compared to other related schemes.

The rest of this paper is organized as follows. Section 2 briefly outlines the related work. The network model, threat model and preliminaries of the proposed TB-CP-ABE are presented in Section 3. Section 4 provides an in-depth and algorithm-wise discussion on the proposed TB-CP-ABE. A formal security analysis is conducted in Section 5. Section 6 undertakes a comparative performance analysis with other related schemes. Conclusions are presented in Section 7.

2 Related Work

Given the diverse number and types of terminals connected to the cloud platform for RES, a flexible control strategy is essential. To address this need, this paper will propose a scheme based on CP-ABE to meet the high scalability scenarios of multiple users in cloud environments. This scheme aims to ensure the stability and security of the cloud while accommodating the access requirements of various terminals.

Due to resource constraints arising from application demands and hardware limitations, terminals connected to RES often struggle to perform the basic operation of the ABE scheme, namely the bilinear pairing operation. Meanwhile, the cloud platform of the RES is supported by edge devices with robust data computing and processing capabilities. Consequently, terminals can offload some decryption tasks to edge devices to alleviate their computational burden. Xue et al. [7] introduced an efficient ABAC scheme, which effectively offloads high computational loads to CSP. However, connecting large-scale terminals to CSP in RES and increasing its burden is not a good solution. Zhang et al. [8] proposed a decentralized scheme that uses a version control subprogram to manage the version of each attribute. However, in a distributed environment, the scheme does not use blockchain for trust or reputation management. Building on Zhang's work, Zhao et al. [9] introduced a data outsourcing access control scheme that offloads operation loads to fog nodes, reducing computational costs. This scheme is suitable for resource-constrained environments but lacks consideration for attribute revocation and device security.

To further improve secure data sharing, Xu et al. [10] developed a data distribution system with cloud-fog-device architecture by delegating the task of identifying data sources to fog nodes. However, it does not propose an algorithm for attribute revocation. In a similar vein, Ge et al. [11] proposed a lightweight CP-ABE scheme based on a trusted billing mechanism. By integrating anonymous authentication and ABAC, this scheme empowers the DO to autonomously determine fine-grained access policies and set the maximum number of accesses for authorized users. Although both schemes effectively outsource high computational loads to CSP, they do not address attribute weighting, resulting in ciphertext being associated solely with attribute-based access policies. Li et al. [12] introduced a weighted access control scheme, wherein the DO assigns weights to attributes to establish a fine-grained access structure. Heavy computational tasks are deferred to the offline stage, resulting in improved weighted access control and increased risk of impersonated terminals.

In contrast, Zhang et al. [13] proposed a secure and lightweight scheme for sharing smart health devices by outsourced verifiable decryption and supporting online/offline encryption and decryption testing. However, the usage of AND gate has brought about complex access structure management. Further exploring this domain, Tao et al. [14] proposed an outsourced attribute encryption scheme called ORR-CP-ABE that allows for reusable decryption results. This system enables outsourcing devices to reuse pre-computed decryption results for subsequent outsourcing requests by transforming keys, thereby reducing the computational burden on the system. Unfortunately, this system does not address trust management and user revocation issues.

Since the properties of terminals in RES may vary due to deployment location, operational duration, and work requirements, the proposed scheme must incorporate property revocation functionality to adapt the access rights of terminals. Xu et al. [15] introduced an efficient and secure ABAC framework, which supports attribute revocation to prevent the extraction of private information through the control matrix. However, due to the lack of outsourced decryption, the terminal computational pressure is heavy. Xiong et al. [16] proposed a signature scheme based on identity. Utilizing a binary tree structure, this scheme ensures secure data communication between data collectors and data analysis systems by achieving attribute revocation. Meanwhile, due to the limited expressive power of binary trees, attribute management and scalability will become very poor. Ma et al. [17] introduced a lightweight, and scalable CP-ABE mechanism, which includes user key revocation, key leakage prevention, and verifiable outsource decryption. However, it relies on a centralized authorization strategy and has complex access structure management.

With the development of blockchain technology and the increasing emphasis on device security, access control schemes based on blockchain have gradually become a research focus. Liu et al. [18] proposed a trading schema using the directed acyclic graph blockchain system based on renewable energy certificates. However, the management authority of the certificate does not belong to the user and IoT devices, so it is not applicable to the context of this article. Feng et al. [19] proposed a policy hiding method integrating CP-ABE and blockchain. The scheme considers trust management of terminals while neglecting attribute revocation, making it inflexible in the IoT environment. Alqbaishi et al. [20] introduced a comprehensive approach that evaluates the requester's reputation with respect to regulating access requests for IoT resources. However, excessive trust management can affect the real-time performance of services. Wei et al. [21] proposed a trustworthy access control method for 6G-multiaccess edge computing networks. But the solution addresses the issues of data sharing between edge devices, not the data access between users and IoT devices discussed in this article.

Despite extensive researches on access control in RES within edge computing environments, the existing schemes fail to fully balance the trust management of devices with the excessive computing pressure. Moreover, in multi-user collaborative computing environments, the dynamism and randomness of terminal behavior make resource access control complex. Trust management theory and blockchain provide effective solutions to these challenges. However, current blockchain solutions either have high trust management costs or only address the issue of data sharing between devices. Therefore, in order to realize the secure sharing of cloud-based data in edge-computing RES, this paper proposes a flexible access control scheme based on trust management, which comprehensively considers attribute revocation and lightweight computing.

3 System Model

3.1 Bilinear Maps

Let G_1 and G_2 be two multiplication cyclic groups of prime order p, and g is a generator of G_1. A map $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map and has the following properties:

1) Bilinearity: for $\forall P, Q \in G$ and $a, b \in Z_p^*$, $e\left(P^a, Q^b\right) = e\left(P, Q\right)^{ab}$;

2) Non-degeneracy: $e\left(g, g\right) \neq 1$;

3) Computability: for $\forall P, Q \in G$, there is an efficient algorithm to compute $e\left(P, Q\right)$.

3.2 LSSS Matrix

A secret sharing scheme across a set of parties P is termed linear (over Z_p) if it satisfies the following conditions:

1) Each party is represented as a vector over Z_p.

2) There exists a matrix M with l rows and n columns, known as the share-generating matrix for the secret sharing scheme. For every $i = 1, 2, \ldots, l$, the ith row of M corresponds to a party $\rho\left(i\right)$ (where ρ is a mapping function from $\{1,\ 2,\ \ldots,\ l\}$ to P). Given the column vector $v = \left(s,\ r_2,\ \ldots,\ r_n\right)$, where $s \in Z_p$ represents the secret to be shared, and $r_2,\ \ldots,\ r_n$ are randomly selected, $M \cdot v$ yields the vector of l shared secrets. The shared secret $\left(M_i \cdot v\right)$ corresponds to party $\rho\left(i\right)$.

Based on the aforementioned description, the linear reconstruction secret sharing scheme can be defined as follows:

Let the access structure A be an LSSS matrix, and let $S \in A$ be any attribute set. Let $I \subset \{1, 2, \ldots, l\}$ be defined as $I \subset \{i\colon \rho\left(i\right) \in S\}$, and then, there exists a constant $\left\{\omega_i \in Z_p\right\}_{i \in I}$. If $\{\lambda_i\}$ satisfies the shared secret value s, then $\sum_{i \in I} \omega_i \lambda_i = s$.

3.3 Decisional q-BDHE Assumption

Based on the system security parameter, the challenger selects two groups G_1 and G_2, where g is the generator of G_1, and the two groups are the prime order p. Let $a, s, b_1, \ldots, b_q \in Z_p$ be obtained arbitrarily. An adversary can be obtained for the following data:

$$\overrightarrow{y} = \begin{pmatrix} g, g^s, g^a, \ldots g^{\left(a^q\right)}, g^{\left(a^{q+2}\right)}, \ldots g^{\left(a^{2q}\right)} \\ \forall_{1 \leq j \leq q} g^{s \cdot b_j}, g^{a/b_j}, \ldots, g^{a^q/b_j}, g^{a^{q+2}/b_j}, \ldots, g^{a^{2q}/b_j} \\ \forall_{1 \leq j,k \leq q, k \neq j} g^{a \cdot s \cdot b_k/b_j}, \ldots, g^{a^q \cdot s \cdot b_k/b_j} \end{pmatrix}. \tag{1}$$

Distinguishing $e\left(g,g\right)^{a^{q+1}s} \in G_T$ from a random element in G_2 is challenging. A challenger $\mathcal{C}$ may guess $z \in \{0,1\}$ with an advantage ε in resolving the decisional q-parallel BDHE when

$$\varepsilon \leq \left|\Pr\left[\mathcal{C}\left(\overrightarrow{y}, T = e\left(g,g\right)^{a^{q+1}\varepsilon}\right) = 0\right] - Pr\left[\mathcal{C}\left(\overrightarrow{y}, T = R\right) = 0\right]\right|. \tag{2}$$

Definition 1: It's inferred that the (decisional) q-parallel BDHE assumption holds if no polytime algorithm has a nonnegligible advantage in solving the decisional q-parallel BDHE problem.

3.4 System Model

The TB-CP-ABE scheme for RES involves five entities: CSP, AA, ES, DO, and DU, each serving specific roles and interactions as described below:

CSP is responsible for storing ciphertexts generated by DO. When ES submits a data access request, CSP validates the access permissions and subsequently delivers the relevant ciphertext to ES.

AA generates the system's public parameters, initializes attributes, and produces a master secret key and public key. DO utilizes the public key for encryption. Upon receiving a request for key generation, AA provides ES with an outsourcing decryption key.

ES utilizes a trust management model to conduct an in-depth analysis of user behavior data, environmental conditions, and other relevant factors, thereby comprehensively assessing the trustworthiness of the data user (DU). To ensure the security of trust scores and device data during transmission and storage, ES employs advanced encryption technologies, safeguarding trust scores and related data from tampering or leakage during transmission. Additionally, ES uploads ciphertexts to CSP and forwards access requests from DU to AA to obtain secret keys. Upon receiving the secret key, ES decrypts the trust threshold, evaluates DU's trust value against the specified threshold, partially decrypts CSP-received ciphertext for DU.

DO defines access structures and encrypts plaintext data using these structures and the public key. ES subsequently sends the ciphertext to CSP for storage and processing.

DU represents RES devices with constrained resources. DU forwards access requests to ES to obtain partially decrypted results, which DU further decrypts to access plaintext data.

3.5 Security Model

The established security model, detailed in Reference [22], will be used to prove the security of the scheme, where a malicious adversary, denoted as $\mathcal{A}$, has the capability to choose an access structure M^* to test the encryption process prior to its ***Setup***. Additionally, $\mathcal{A}$ is granted the authority to request any user private key associated with an attribute set L that does not comply with M^* $(L| \neq M^*)$. The primary goal of $\mathcal{A}$ is to obtain the encryption keys utilized in ***Encrypt*** and subsequently decrypt any newly encrypted messages using those keys. Apart from the malicious adversary $\mathcal{A}$, there is not complete trust in all entities within the system, and they may potentially engage in eavesdropping or tampering attacks. Based on the assumptions above, AA is the only entity considered fully trustworthy, while CSP and ES are regarded as partially trusted. This implies that although they perform the protocol honestly, they may still have a curiosity regarding the secret of other entities. Consequently, the game will be outlined as follows:

1) *Initialization*: $\mathcal{A}$ selects an access structure M^* for the challenge and submits it to the challenger $\mathcal{C}$.

2) *Setup*: $\mathcal{C}$ performs the *Setup* procedure to generate the public parameters PP. The public key PK and public parameters PP are provided to $\mathcal{A}$, while MSK remains confidential.

3) *Phase 1*: $\mathcal{A}$ generates an attribute set L, where $L| \neq M^*$ and requests an outsourced decryption key of L from $\mathcal{C}$. In response, $\mathcal{C}$ generates relevant keys based on the attribute set, identity, and private key provided by $\mathcal{A}$, which is called $SK_{ES,GID_{DU}}$. These queries will be made iteratively.

4) *Challenge*: $\mathcal{A}$ transmits two messages msg_0 and msg_1 of same length to $\mathcal{C}$. Subsequently, $\mathcal{C}$ randomly selects h from $\{0, 1\}$ and encrypts $msg_h \in \{msg_0,\ msg_1\}$ under M^* to obtain ciphertext CT^* and sends it to $\mathcal{A}$.

5) *Phase 2*: *Phase 1* is repeated under the condition that none of the attribute sets adhere to the access structure M^*.

6) *Guess*: $\mathcal{A}$ presents its guess h' for h.

The advantage ε_{Adv} of the challenger $\mathcal{C}$ is defined as $\Pr\left[\mathcal{C}\left(Y, T = e(g,g)^{a^{q+1}\varepsilon}\right) = 0\right] - \Pr\left[\mathcal{C}(Y, R) = 0\right]$.

Definition 2: A CP-ABE scheme is deemed CPA-secure if no adversary can gain a significant advantage in winning the CPA-CP-ABE game within polynomial time.

3.6 Threat Model

Assuming the KGC is a fully trusted entity, it generates the system parameters and securely distributes encryption and decryption keys to other entities through secure channels. The CSP is considered semi-trusted, faithfully executing system operations but potentially capable of launching passive attacks. DUs are untrustworthy and may initiate any type of attack. As receivers, DUs may attempt to decrypt unauthorized ciphertexts. As senders, they might impersonate unauthorized senders by generating messages to others. For simplicity, unauthorized parties refer to colluding entities among CSP, ESs, and DUs who lack valid decryption and encryption keys. Below is a summary of potential attacks in RES system:

Insider Attack: Insider attacks arise when authorized users exploit their legitimate access to circumvent access policies. They may manipulate their attributes, steal decryption keys, or exploit system vulnerabilities to decrypt or modify sensitive data. This unauthorized access undermines system security, necessitating rigorous monitoring, audits, and user training to mitigate risks.

Impersonation Attack: In an impersonation attack, any party can mimic an encryption key with unauthorized attributes or craft ciphertexts by attaching unauthorized sender's attributes, misleading receivers. Furthermore, having obtained a valid ciphertext, unauthorized parties might attempt to replace or modify the underlying message to impersonate the corresponding sender.

Collusion Attack: Unauthorized parties can collaborate to launch the aforementioned attacks. For instance, they may combine multiple decryption keys to decrypt unauthorized ciphertexts or exchange encryption keys to generate ciphertexts without authorizing the sender's attributes.

Distributed Denies of Service (DDoS) Attack: DDoS attacks can overwhelm the system by flooding it with requests from multiple sources, exploiting authorized users' devices or hijacked resources. This overwhelms the servers, degrades performance, and potentially denies legitimate users access to encrypted data and services, disrupting the secure data sharing ecosystem.

4 Proposed Scheme

The TB-CP-ABE scheme for the edge-computing-assisted REIoT is presented in this section. The TB-CP-ABE scheme includes seven algorithms: ***Setup***, ***AASetup***, ***Encrypt***, ***KeyGen***, ***ESDec***, ***DUDec***, and ***AttrRevo***. At the beginning, KGC runs ***Setup*** to select total system parameters, and AA runs ***AASetup*** to pick public key and private key. DO is required to run the ***Encrypt*** algorithm to prescribe the generation of Linear Secret Sharing Scheme (LSSS) matrix and decryption material, encrypt and upload data to the cloud. When DU intends to download data encrypted by DO, DU can submit a request to AA. Subsequently, AA performs the ***KeyGen*** to produce the attribute key tailored to DU's specific attributes. Then, ES is tasked with running ***ESDec*** to decrypt the trust threshold necessary for the plaintext and evaluate whether the DU's trust level exceeds this threshold. If so, ES proceeds with decrypting part of the encrypted data and transmitting the data to DU. After DU executes ***DUDec*** to complete the final decryption, DU obtains the plaintext data. As DU's attributes may vary based on geographical location, working hours, and security level, this TB-CP-ABE also incorporates ***AttrRevo*** algorithm to revoke the expired attributes associated with DU. The notations used in TB-CP-ABE is listed in Table 2 and the overall negotiation process is shown in Fig. 1 and the trust evaluation process is shown in Fig. 2 below.

Table 2: Notations used in TB-CP-ABE

Symbol	Description	Symbol	Description
PP_{Setup}	Public parameter	sk_{DU}	Private key of DU
$attr_i$	ith attribute	T_m	Trust threshold defined by DO
MSK	Master private key used by AA to generate private key	T_{ES}	Encrypted trust threshold
PK	Public key used by DO/DU/ES	CT	Encrypted data and decryption material uploaded to CSP
(M, ρ)	LSSS matrix defined by DO	$SK_{ES,GID_{DU}}$	Outsourced decryption key used by ES
ε	Secret value	TK_{ES}	Trust decryption key used by ES
m	Plaintext	A	Decryption material calculated by ES
$C_0, C_1, \left\{C_{2,i}, C_{3,i}\right\}_{\forall i\in[1,n]}$	Decryption material generated by DO	CT'	Partially decrypted ciphertext generated by ES

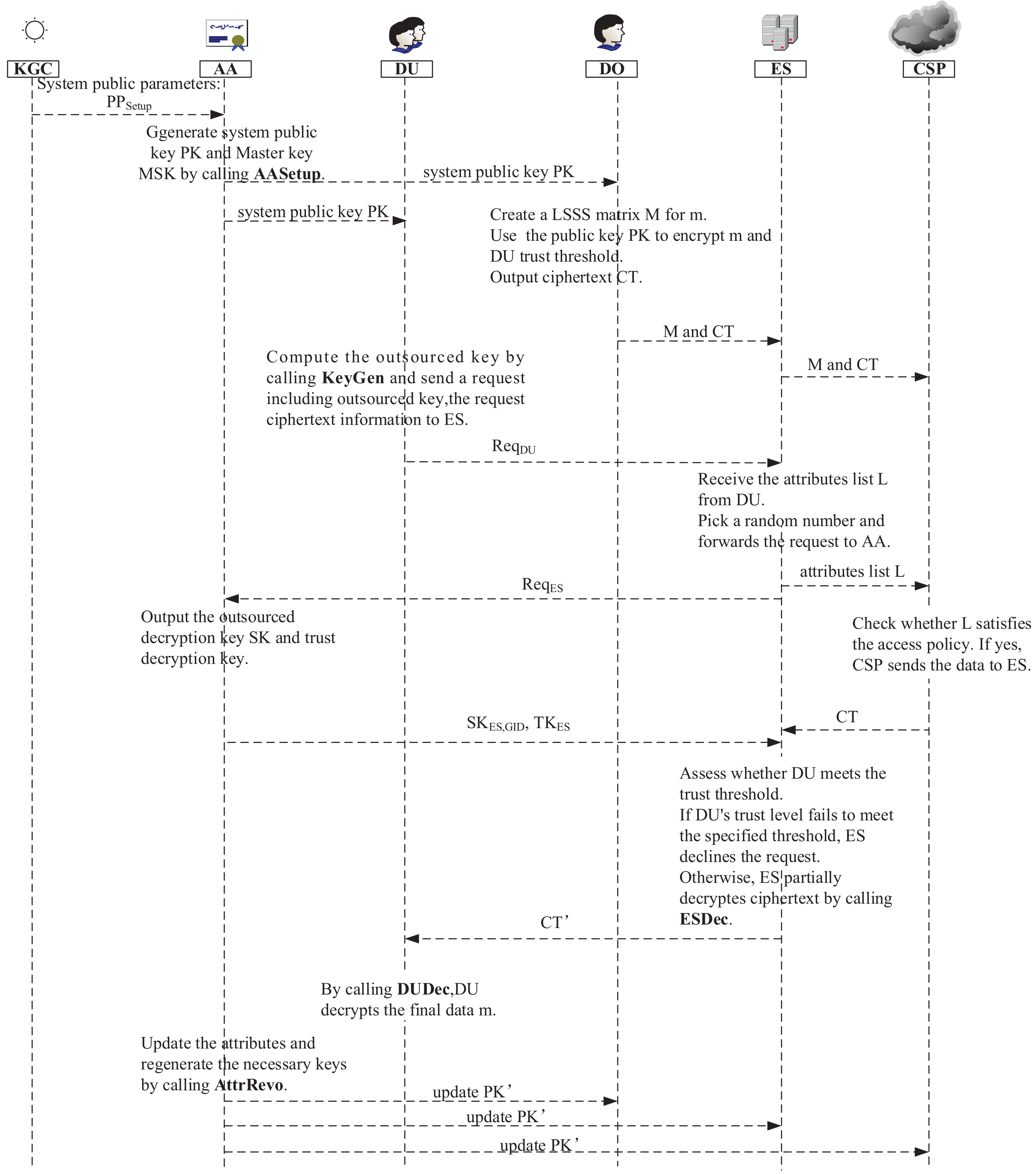
KGC
AA
DU
DO
ES
CSP
System public parameters:
PP_{Setup}
Ggenerate system public
key PK and Master key
MSK by calling **AASetup**.
system public key PK
system public key PK
Create a LSSS matrix M for m.
Use the public key PK to encrypt m and
DU trust threshold.
Output ciphertext CT.
M and CT
M and CT
Compute the outsourced key by
calling **KeyGen** and send a request
including outsourced key,the request
ciphertext information to ES.
Req_{DU}
Receive the attributes list L
from DU.
Pick a random number and
forwards the request to AA.
attributes list L
Req_{ES}
Output the outsourced
decryption key SK and trust
decryption key.
Check whether L satisfies
the access policy. If yes,
CSP sends the data to ES.
CT
$SK_{ES,GID}$, TK_{ES}
Assess whether DU meets the
trust threshold.
If DU's trust level fails to meet
the specified threshold, ES
declines the request.
Otherwise, ES partially
decryptes ciphertext by calling
ESDec.
CT’
By calling **DUDec**,DU
decrypts the final data m.
Update the attributes and
regenerate the necessary keys
by calling **AttrRevo**.
update PK’
update PK’
update PK’

Figure 1: Access control phase in the proposed TB-CP-ABE

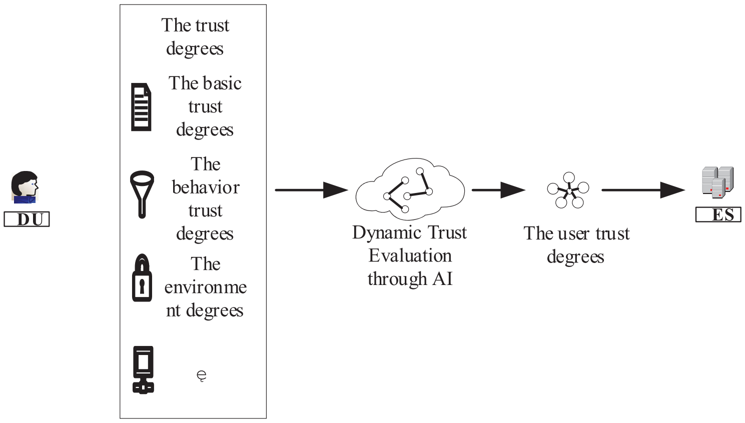

Figure 2: The trust evaluation process in the proposed TB-CP-ABE

4.1 Setup

In the Setup phase, the system initializes the essential parameters required for encryption and decryption. Security parameter δ_{sp} is taken as input, and PP_{Setup} is taken as output. KGC selects two multiplicative cyclic groups G_1 and a generator g of G_1, where p is the prime order of group G_1. Then, KGC selects a bilinear map $e\colon\ G_1 \times G_1 \to G_2$ and a hash function $H\colon\ \{0,\ 1\}^* \to G_1$. The TB-CP-ABE scheme's public parameters are outlined as

$$PP_{Setup} = (p,\ G_1,\ G_2,\ e,\ g,\ H)\,. \tag{3}$$

4.2 AASetup

In the AASetup phase, the attribute field Q of the system and the public parameters PP_{Setup} are primarily taken as inputs, and the master private key MSK of AA and the public key PK are taken as outputs. AA selects two random number $\sigma \in Z_p^*$, $\eta \in Z_p^*$ and generates $pk_1 = e(g,\ g)^{\sigma}$ and $pk_2 = g^{\sigma} pk_3 = e(g,\ g)^{\eta}$, $pk_4 = g^{\eta}$. For each attribute $attr_i \in Q$, AA randomly selects $\beta_1,\ \beta_2,\ \cdots \beta_i,\ \cdots \beta_n \in Z_p \quad n = len(Q)$, and computes $pk_5 = g^{-\sigma\beta_i}$.The master private key MSK of AA and the public key PK are generated as

$$MSK = \{\sigma, \{\beta_i\}\} \tag{4}$$

$$PK = \left\{\left(pk_{1,}\ pk_{2,}\ pk_{3,}\ pk_{4,}\ pk_5\right) = \left(e(g,\ g)^{\sigma},\ g^{\sigma},\ e(g,\ g)^{\eta},\ g^{\eta},\ g^{-\sigma\beta_i}\right)\right\} \tag{5}$$

4.3 Encrypt

In the Encrypt phase, DO runs the algorithm to encrypt the plaintext m. The plaintext m, the public parameters PP_{Setup} and the LSSS matrix (M, ρ) are taken as inputs, CT is taken as outputs. DO constructs a LSSS matrix $(M,\ \rho)$ for the plaintext m. It selects a random vector $\overrightarrow{k} = (\varepsilon,\ k_2,\ k_3,\ \ldots, k_n)^T \in Z_p^*$ where ε is secret value and calculates a sharing vectors as $(\lambda_1, \ldots, \lambda_i,\ \ldots,\ \lambda_n)^T = \overrightarrow{k} M$. Then, DO calculates decryption material as $C_0 = m \cdot \left(\prod_{pk_1 \in PK_M} pk_1\right)^{\varepsilon} = m \cdot e(g, g)^{\sigma\varepsilon}$, $C_1 = g^{\varepsilon}$. For $i \in [1, n]$, $C_{2,i} = g^{\lambda_i}$, $C_{3,i} = \left(\prod_{pk_3 \in PK_M} pk_3\right)^{\varepsilon} = \prod\limits_{attr_i \in Q} g^{-\sigma\beta_i\varepsilon}$. Finally, DO selects the DU trust threshold T_m that can be decrypted, encrypts the threshold as $T_{ES} = T_m \cdot (pk_3)^{\varepsilon} = T_m \cdot e(g,g)^{\eta\varepsilon}$, and outputs CT as

$$CT = \left\{(M,\rho), C_0, C_1, \left\{C_{2,i}, C_{3,i}\right\}_{\forall i \in [1,n]}, T_{ES}\right\}. \tag{6}$$

4.4 KeyGen

In the KeyGen phase, the attributes list from Req, master private key MSK and the public parameters PP_{Setup} are taken as inputs, the outsourced decryption key $SK_{ES,GID_{DU}}$ is taken as outputs. DU picks secret key $\theta_{DU} \in Z_p^*$ randomly, and generates $g^{\theta_{DU}}$ and $sk_{DU} = \frac{1}{\theta_{DU}}$. Then, DU packs secret material $Req_{DU} = \{GID_{DU}, g^{\theta_{DU}}, L\}$ and sends it to ES. Upon receiving the attributes list from Req, ES picks a random number r_{ES} and forwards the request $Req_{ES} = \{GID_{DU}, g^{\theta_{DU}}, L, g^{r_{ES}}\}$ to AA. AA outputs the outsourced decryption key $SK_{ES,GID_{DU}} = g^{\lambda_i\theta_{DU}} H(GID_{DU})^{\lambda_i\beta_i}$ and trust decryption key $TK_{ES} = pk_4 \cdot g^{r_{ES}} = g^{\eta} \cdot g^{r_{ES}}$ and sends them to the corresponding ES.

4.5 ESDec

In the ESDec phase, the public parameters PP_{Setup} are taken as inputs, the encrypted data CT and the outsourced decryption key $SK_{ES,GID_{DU}}$ are taken as outputs. When ES receives a data request from DU, ES applies to the CSP for downloading data ciphertext CT. CSP initially verifies the existence of a subset $L' = \{i\colon \rho(i) \in S\} \subset L$. If DU's attributes meet decryption requirements, ES calculates $\left\{\omega_i \in Z_p\right\}$. If not, CSP denies the request. According to the properties of LSSS matrix M, the shared secret value ε can be obtained by $\sum_{i\in L'} \omega_i\lambda_i = \varepsilon$. Then, ES decrypts T_m as

$$\begin{aligned} A &= \frac{e(C_1, TK_{ES})}{\prod_{i\in L'}\left(e\left(C_{2,i}, g^{r_{ES}}\right)\right)^{\omega_i}} = \frac{e(g^{\varepsilon}, g^{\eta}\cdot g^{r_{ES}})}{\prod_{i\in L'}\left(e(g^{\lambda_i}, g^{r_{ES}})\right)^{\omega_i}} \\ &= \frac{e(g^{\varepsilon}, g^{\eta}) \cdot e(g^{\varepsilon}, g^{r_{ES}})}{e(g^{\varepsilon}, g^{r_{ES}})} = e(g,g)^{\eta\varepsilon} \end{aligned} \tag{7}$$

$$T_m = \frac{T_{ES}}{A} = \frac{T_m \cdot e(g,g)^{\eta\varepsilon}}{e(g,g)^{\eta\varepsilon}}. \tag{8}$$

As ES gathers data including DU's application resource success rates, attribute details, and attribute update frequency to gauge DU's trustworthiness, it can compare DU's trust level with the trust threshold necessary for accessing the data. If DU's trust level fails to meet the specified threshold, ES will decline the delivery of encrypted packets to DU. Otherwise, ES will assist DU by decrypting a portion of the ciphertext to alleviate the decryption burden on DU and send CT' to DU as

$$\begin{aligned} CT' &= \prod_{i\in L'}\left\{e\left(pk_2{}^{\omega_i}, SK_{ES,GID_{DU}}\right) \cdot e\left(H(GID_{DU}), C_{3,i}\right)\right\} \\ &= e(g,g)^{\sum_{i\in L'} \sigma\lambda_i\omega_i\theta_{DU}} = e(g,g)^{\sigma\varepsilon\theta_{DU}}. \end{aligned} \tag{9}$$

4.6 DUDec

DU only requires basic operations to decrypt the plaintext m as

$$m = \frac{C_0}{CT'sk_{DU}} = \frac{m \cdot e(g,g)^{\sigma\varepsilon}}{\left(e(g,g)^{\sigma\varepsilon\theta_{DU}}\right)^{\frac{1}{\theta_{DU}}}}. \tag{10}$$

4.7 AttrRevo

Due to the variability of DU's attributes, influenced by factors such as geographical location and security level, the scheme needs to support for specific attribute revocation. The output of this algorithm is β_i that needs to be updated, and the related PK, $SK_{ES,GID_{DU}}$, and $C_{3,i}$. First, AA reselects β_i' as an attribute random number, and updates PK as

$$PK' = \left\{\left(pk_1, pk_2, pk_3{}'\right) = \left(e\left(g,g\right)^{\sigma}, g^{\sigma}, g^{-\sigma\beta_i{}'}\right)\right\}. \tag{11}$$

Then, AA regenerates outsourced decryption key $SK_{ES,GID_{DU}}$ for ES as

$$SK_{ES,GID_{DU}}{}' = \left(g^{\theta_{DU}}\right)^{\sigma-\sigma\frac{\beta_i'}{\beta_i}} \cdot SK_{ES,GID_{DU}}{}^{\frac{\beta_i'}{\beta_i}}. \tag{12}$$

Finally, AA updates decryption material $C_{3,i}$ and CT to DO, CSP and ES as

$$C_{3,i}{}' = C_{3,i} \cdot C_1{}^{\beta_i-\beta_i{}'} = \left(\prod_{pk_3\in PK_M} pk_3\right)^{\varepsilon} \cdot g^{\sigma\cdot\left(\beta_i-\beta_i{}'\right)} = \prod_{attr_i\in Q} g^{-\sigma\beta_i\varepsilon} \cdot g^{\sigma\cdot\left(\beta_i-\beta_i{}'\right)} \tag{13}$$

$$CT' = \left\{\left(M,\rho\right), C_0, C_1, \left\{C_{2,i}, C_{3,i}{}'\right\}_{\forall i\in[1,n]}, T_{ES}\right\}. \tag{14}$$

After updating the three parameters above, the specific attribute is revoked.

5 Security Analysis

Theorem 1: Assuming the decisional *q-BDHE* assumption is valid, it follows that no adversary can undermine the proposed scheme within probabilistic polynomial-time when confronted with the challenge involving a specified access structure M^*.

Proof: Assume the existence of an adversary $\mathcal{A}$ with a non-negligible advantage $Adv_{\mathcal{A}}$ in the cracking TB-CP-ABE scheme. Furthermore, suppose that $\mathcal{A}$ generates an access structure M^* for challenge. Proceed to demonstrate the construction of a challenger $\mathcal{C}$, which engages in solving the decisional *q-BDHE* problem.

1) *Initialization*: The challenger $\mathcal{C}$ receives the access structure M^* from $\mathcal{A}$. Represent the attribute value within M^* by $\mathcal{V}^* = \{v_1, v_2, \ldots, v_l\}$, where l signifies the length of attributes in M^*.

2) *Setup*: The challenger $\mathcal{C}$ performs the ***Setup*** and subsequently forwards PP_{Setup} and PK to $\mathcal{A}$. Following this, $\mathcal{C}$ picks several random numbers $rn^* \in \{1, 2, \ldots, l\}$, $\sigma \in Z_p^*$, $\eta \in Z_p^*$ and $\beta_i' \in Z_p^*$ for the ith attribute $attr_i$. For $\mathcal{I}^* = \{1, 2, \ldots, l\}$ and $rn \in \mathcal{I}^*$, $\mathcal{C}$ selects $\beta_{v_{rn}} \in Z_p^*$ for the related attribute.

For $rn \in \mathcal{I}^*$ and $rn \neq rn^*$, $\mathcal{C}$ calculates pk_1, pk_3, pk_5 in PK as follows:

1) If $attr_i = M^*_{v_{rn}}$, $\mathcal{C}$ calculates $pk_{1,v_{rn}} = e\left(g,g\right)^{\sigma}$, $pk_{3,v_{rn}} = e\left(g,g\right)^{\eta}$ and $pk_{5,v_{rn}} = g^{\sigma\beta_{v_{rn}}} \cdot g^{\left(a^{q+1-v_{rn}}\right)^{-1}}$.

2) If $attr_i \neq M^*_{v_{rn}}$, $\mathcal{C}$ calculates $pk_1 = e\left(g,g\right)^{\sigma}$, $pk_3 = e\left(g,g\right)^{\eta}$ and $pk_5 = g^{-\sigma\beta_i{}'}$.

For $rn \in \mathcal{I}^*$ and $rn = rn^*$, $\mathcal{C}$ calculates pk_1, pk_3, pk_5 in PK as follows:

3) If $attr_i = M^*_{v_{rn}}$, $\mathcal{C}$ calculates $pk_{1,v_{rn^*}} = e\left(g,g\right)^{\sigma}$, $pk_{3,v_{rn^*}} = e\left(g,g\right)^{\eta}$ and $pk_{5,v_{rn^*}} = g^{\sigma\beta_{v_{rn}}} \cdot g^{a^{q+1-v_{rn}}}$.

4) If $attr_i \neq M^*_{v_{rn}}$, $\mathcal{C}$ refers to (2) and calculates them.

For $rn \notin \mathcal{I}^*$, $\mathcal{C}$ refers to (2) and calculates them.

3) *Phase 1*: $\mathcal{C}$ responds to $\mathcal{A}$'s inquiries for the master key MSK, outsourced decryption key $SK_{ES,GID_{DU}}$ and trust decryption key TK_{ES} for the attribute set L, deviates from the access structure M^*.

The adversary $\mathcal{A}$ provides a identity random number GID_{DU} and an attributes list L to ask for a ***KeyGen*** query. The challenger $\mathcal{C}$ establishes a random oracle table $\mathcal{H}$ to record all the query results. During the initialization process, all system entities share the random oracle $\mathcal{H}$, denoted as $\mathcal{H}(x)$. Each time $\mathcal{A}$ submits the identity random number GID_{DU} to $\mathcal{C}$ in a query, if $\mathcal{H}(GID_{DU})$ is available, $\mathcal{C}$ simply responds the previous response. Otherwise, $\mathcal{C}$ selects a random value $t \in Z_p^*$ and sets $\mathcal{H}(GID_{DU}) = g^{a^{v_{rn}'}} \cdot g^t$.

For $attr_{v_{rn'}}$, $\mathcal{C}$ computes the outsourced decryption key as $SK_{v_{rn}',GID_{DU}} = g^{\sigma\theta_{DU}} \cdot \mathcal{H}(GID_{DU})^{\beta_i'}$.

For $rn \neq rn'$, $\mathcal{C}$ computes the outsourced decryption key as follows:

(1) If $rn \in \mathcal{I}^*$ and $v_{rn} \in \mathcal{V}^* - v_{rn}{}^*$, $\mathcal{C}$ calculates $SK_{v_{rn},GID_{DU}} = g^{\sigma\theta_{DU}} \cdot \left(g^{a^{v_{rn}'}}\right)^{-\sigma\beta_{v_{rn}}'} \cdot g^{a^{q+1-v_{rn}+v_{rn}'}} \cdot pk_{5,v_{rn}}{}^{-t}$. From this, $\mathcal{A}$ can decrypt $pk_{1,v_{rn}}$

$$\begin{aligned} & e\left(SK_{v_{rn},GID_{DU}}, g\right) \cdot e\left(\mathcal{H}(GID_{DU}), pk_{5,v_{rn}}\right) \\ & \cdot e(g,g)^{a^{v_{rn}'} \cdot \sigma\beta_{v_{rn}}} \cdot e(g,g)^{\left(a^{v_{rn}'} \cdot a^{q+1-v_{rn}}\right)^{-1}} \cdot e\left(pk_{5,v_{rn}}, g^t\right) \\ & = e(g,g)^{\sigma\theta_{DU}} = pk_{1,v_{rn}}{}^{\theta_{DU}}. \end{aligned} \tag{15}$$

(2) If $rn \in \mathcal{I}^*$ and $rn = rn^*$, $\mathcal{C}$ calculates $SK_{v_{rn}*,GID_{DU}} = g^{\sigma\theta_{DU}} \cdot \left(g^{a^{v_{rn}'}}\right)^{-\sigma\beta_{v_{rn}'}} \cdot g^{\left(a^{q+1-v_{rn}+v_{rn}'}\right)^{-1}} \cdot pk_{5,v_{rn}*}{}^{-t}$. From this, $\mathcal{A}$ can decrypt $pk_{1,v_{rn}*}$ as

$$\begin{aligned} & e(SK_{v_{rn}*,GID_{DU}}, \mathrm{g}) \cdot \mathrm{e}(\mathcal{H}(\mathrm{GID}_{DU}), pk_{5,v_{rn}*}) \\ & = \mathrm{e}(g^{\sigma\theta_{DU}} \cdot (g^{a^{v_{rn}'}})^{-\sigma\beta_{v_{rn}'}} \cdot g^{(a^{q+1-v_{rn}+v_{rn}'})^{-1}} \cdot pk_{5,v_{rn}*}{}^{-t}, g) \cdot e(g^{a^{v_{rn}'}} \cdot g^t, pk_{5,v_{rn}*}) \\ & = e(g,g)^{\sigma\theta_{DU}} = pk_{1,v_{rn}*}{}^{\theta_{DU}}. \end{aligned} \tag{16}$$

(3) If $rn \notin \mathcal{I}^*$ and $attr_i \notin M^*$, $\mathcal{C}$ calculates $SK_{rn,GID_{DU}} = g^{\sigma\theta_{DU}} \cdot (H(GID_{DU}))^{-\sigma\beta_{v_{rn}}'}$.

The challenger $\mathcal{C}$ replies to $\mathcal{A}$ with the outsourced decryption key $SK_{*,GID_{DU}}$ and the trust decryption key TK_* for L.

4) *Challenge*: $\mathcal{A}$ transmits two messages msg_0 and msg_1 of the equal length to challenger $\mathcal{C}$ for the challenge ciphertext. Subsequently, $\mathcal{C}$ randomly picks h from $\{0, 1\}$ and generates $msg_h \in \{msg_0, msg_1\}$. Eventually, the complete ciphertext is as follows:

$$\begin{aligned} & C_0{}^* = msg_h \cdot T \cdot \left(\prod_{pk_1 \in PK_M} pk_1\right)^{\varepsilon} \\ & C_1{}^* = g^{\varepsilon} \\ & C_{2,i}{}^* = g^{\lambda_i} \\ & C_{3,i}{}^* = \left(\prod_{rn \in \mathcal{I}^*} pk_3\right)^{\varepsilon} = \prod_{rn \in \mathcal{I}^*} g^{-\sigma\beta_{v_{rn}}{}^*\varepsilon} \\ & CT^* = \left\{(M,\rho), C_0{}^*, C_1{}^*, \left\{C_{2,i}{}^*, C_{3,i}{}^*\right\}_{\forall i \in [1,n]}, T_{ES}\right\}. \end{aligned} \tag{17}$$

5) *Phase 2*: This phase resembles *Phase 1*.

6) *Guess*: For h, $\mathcal{A}$ presents its guess h'. If $h = h'$, the challenger $\mathcal{C}$ demonstrates that $T = e(g,g)^{a^{q+1}\varepsilon}$. Otherwise, it assumes T is a random choice from G_2. If T is randomly chosen from G_2, the adversary $\mathcal{A}$ has no knowledge about the message msg_h. If the challenge ciphertext is valid, which the advantage is ε_{Adv}

$$Pr\left[\mathcal{C}(\mathrm{y}, \mathrm{T} = \mathrm{e}(\mathrm{g},\mathrm{g})^{a^{q+1}\varepsilon} = 0\right] = \frac{1}{2} + \varepsilon_{Adv}. \tag{18}$$

Consequently, the challenger $\mathcal{C}$‘s probability of winning this game is

$$\begin{aligned} Adv_{\mathcal{A}} = &\frac{1}{2}Pr\left[\mathcal{C}\left(y, T = e(g,g)^{a^{q+1}\varepsilon}\right) = 0\right] \\ &+ \frac{1}{2}\Pr\left[\mathcal{C}(y, T = R) = 0\right] - \frac{1}{2} \\ &= \frac{1}{2}\cdot\left(\frac{1}{2} + \varepsilon_{Adv}\right) + \frac{1}{2}\cdot\frac{1}{2} - \frac{1}{2} = \frac{\varepsilon_{Adv}}{2}. \end{aligned} \tag{19}$$

Upon the above proof, it becomes evident that if $\mathcal{A}$ possesses a non-negligible advantage within the security model to break TB-CP-ABE scheme, then $\mathcal{C}$ can likewise break the *q-BDHE* hypothesis with the identical advantage. Hence, it is proved that TB-CP-ABE scheme is secure under the *q-BDHE* assumption.

6 Performance Analysis

6.1 Computational Costs Comparison

For calculating the computational costs during access control phase, it's assumed that the notations T_{bp}, T_{eG}, T_{eG_T}, $|S_u|$, ξ, $|\xi|$, l denote the operation time of a bilinear pairing, a group exponentiation in G, a group exponentiation in G_T, the size of a user attribute set S_u, an minimum rowset in LSSS matrix that the user's attributes satisfy the access policy, the size of rowset ξ, the number of the rows of the LSSS matrix, respectively. Due to variations in operation time across different devices for the same operation, experiment has chosen a Raspberry PI 3 to simulate DU, and a 3 GHz Pentium IV PC to simulate DO, AA and ES, respectively. The corresponding operation time is presented in Table 3. Since DUs in RES scenarios are typically resource-constrained devices, reducing their computational burden is more critical than reducing the computational load on ES, which possess significant computing power. Thus, the computational cost of TB-CP-ABE scheme on DO and DU are 41.8 ms and 3.52 ms, respectively, which is superior to other relevant schemes as tabulated in Table 4.

Table 3: Execution time of various cryptographic operations

Operation	Raspberry PI 3	Pentium IV
T_{bp}	30.67 ms	12.28 ms
T_{eG}	15.62 ms	2.61 ms
T_{eG_T}	3.52 ms	0.24 ms

Table 4: The computational cost of algorithms

Schemes	***KeyGen*** cost	***Encrypt*** cost	***ESDec*** cost	***DUDec*** cost
[23]	$6\|S_u\|T_{eG} = 15.66$ ms	$5T_{eG_T} + 2lT_{eG_T} + 5lT_{eG} =$ 102.74 ms	$\|\xi\|T_{eG_T} + 4\|\xi\|T_{bp} = 49.36$ ms	$\mathrm{T}_{eG} = 15.62$ ms
[24]	$2\|S_u\|T_{eG} = 5.22$ ms	$T_{eG_T} + 2lT_{eG_T} + 3lT_{eG} =$ 57.42 ms	$3\|\xi\|T_{eG_T} + 2\|\xi\|T_{bp} =$ 25.28 ms	$T_{eG} = 15.62$ ms
[25]	$4\|S_u\|T_{eG} = 10.44$ ms	$T_{eG_T} + 2lT_{eG_T} + 3lT_{eG} =$ 57.42 ms	$2\|\xi\|T_{bp} + 3\|\xi\|T_{eG_T} =$ 25.28 ms	$T_{eG_T} = 3.52$ ms
[26]	$4\|S_u\|T_{eG} = 10.44$ ms	$T_{eG_T} + 2lT_{eG_T} + 4lT_{eG} =$ 73.04 ms	$3\|\xi\|T_{bp} + \|\xi\|T_{eG_T} = 37.08$ ms	$T_{eG_T} = 3.52$ ms
[27]	$2\|S_u\|T_{eG} = 5.22$ ms	$T_{eG_T} + 2lT_{eG_T} + 3lT_{eG} =$ 57.42 ms	$3\|\xi\|T_{bp} + 4\|\xi\|T_{eG_T} = 37.8$ ms	$T_{eG_T} = 3.52$ ms
[28]	$2\|S_u\|T_{eG} = 5.22$ ms	$T_{eG_T} + 2lT_{eG_T} + 2lT_{eG} =$ 53.9 ms	$3\|\xi\|T_{bp} + 4\|\xi\|T_{eG_T} = 37.8$ ms	$T_{eG_T} = 3.52$ ms
TB-CP-ABE	$2\|S_u\|T_{eG} = 5.22$ ms	$T_{eG} + 2T_{eG_T} + 2lT_{eG} =$ 41.8 ms	$\|\xi\|T_{bp} + T_{bp} + 2\|\xi\|T_{eG} + T_{eG_T} = 30.02$ ms	$T_{eG_T} = 3.52$ ms

6.2 Communicational Costs Comparison

For calculating the communication costs during access control phase, it's assumed that a random number, an elliptic curve point, an AES ciphertext are 32, 384 and 32 bytes, respectively. The proposed scheme includes private key size and ciphertext size with the communication costs of 384 bytes and 1536 bytes, respectively, totaling 1920 bits. The communication costs of Sethi et al. [23], Zhang et al. [24], Huang et al. [25], Tu et al. [26], Fugkeaw et al. [27], Fugkeaw et al. [28] are 3840, 1538, 2688, 2688, 3104, 3104 bytes respectively as provided in Table 5. It is clear that TB-CP-ABE scheme achieves a substantial reduction in communication overhead compared to the majority of existing schemes.

Table 5: The communicational cost of schemes

Schemes	Private Key Size	Ciphertext Size
[23]	$4\|S_u\|\|G\| = 1536$ bytes	$\|G_T\| + l\|G_T\| + 4l\|G\| = 2304$ bytes
[24]	$\|S_u\|\|G\| = 384$ bytes	$l\|G_T\| + 2l\|G\| + l_1 + l_2 = 1154$ bytes
[25]	$2\|S_u\|\|G\| = 768$ bytes	$l\|G_T\| + 3l\|G\| + \|G_T\| = 1920$ bytes
[26]	$2\|S_u\|\|G\| = 768$ bytes	$l\|G_T\| + 3l\|G\| + \|G_T\| = 1920$ bytes
[27]	$2\|S_u\|\|G\| = 768$ bytes	$2l\|G_T\| + 3l\|G\| + \|G_T\| + \|AES\| = 2336$ bytes
[28]	$2\|S_u\|\|G\| = 768$ bytes	$2l\|G_T\| + 3l\|G\| + \|G_T\| + \|AES\| = 2336$ bytes
TB-CP-ABE	$\|S_u\|\|G\| = 384$ bytes	$\|G_T\| + 2l\|G\| + \|G\| = 1536$ bytes

6.3 Performance Comparison of Algorithms

(1) Computational Performance: To assess the practical feasibility and computational performance of the TB-CP-ABE scheme, experiments are conducted to focus on three key algorithms: ***KeyGen***, ***Encrypt***, and ***ESDec***. The increasing prevalence of ABE in various applications necessitates an understanding of its performance characteristics under varying attribute set sizes. Hence, this

empirical investigation aims to elucidate how the execution times of these algorithms are affected by the growth in attribute complexity. The results are depicted in Figs. 3–5, where the x-axis represents the number of the user attributes ranging from 0 to 30, and the y-axis represents the time (in milliseconds) required for encryption operations. As the size of the user attribute set increases, all five schemes show an overall upward trend, indicating an increase in encryption complexity and therefore requiring longer computation time. However, it can be clearly seen that as the attribute set increases, the proposed scheme does not significantly increase the operation time of ***KeyGen***, ***Encrypt***, and ***ESDec*** algorithms, which proves that TB-CP-ABE outperforms the other four schemes in terms of encryption performance.

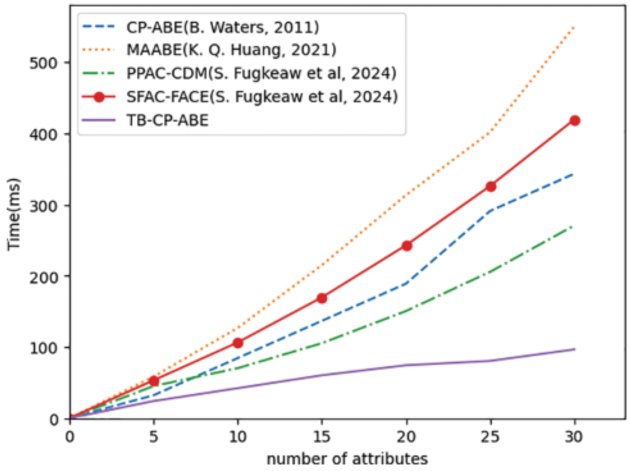

Figure 3: Performance of *KeyGen* [22,25,27,28]

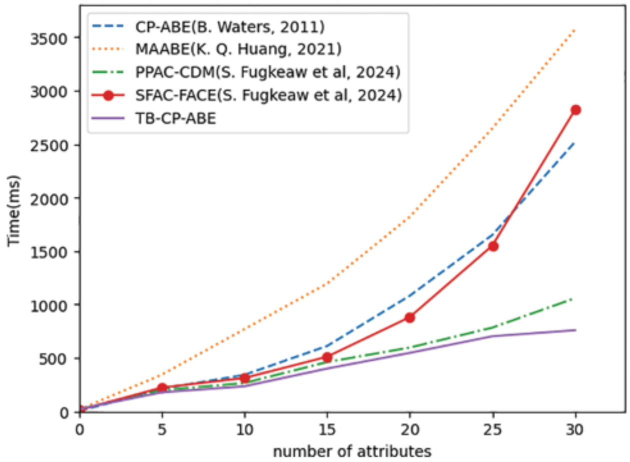

Figure 4: Performance of *Encrypt* [22,25,27,28]

(2) Energy Consumption: In order to understand the energy consumption of different algorithms in different devices, 14 nodes were selected for testing, including 4 high-performance nodes to simulate ESs and 10 low performance nodes to simulate DUs. The 14 nodes on the x-axis in the Fig. 6 are arranged in order of computing power, and the y-axis represents energy consumption (in kWh). From the graph, it can be seen that the TB-CP-ABE scheme has the lowest computational cost in both

high-performance and low performance nodes. This is consistent with the analysis of computational and communication costs, and the proposed solution has good performance, reducing the burden on devices.

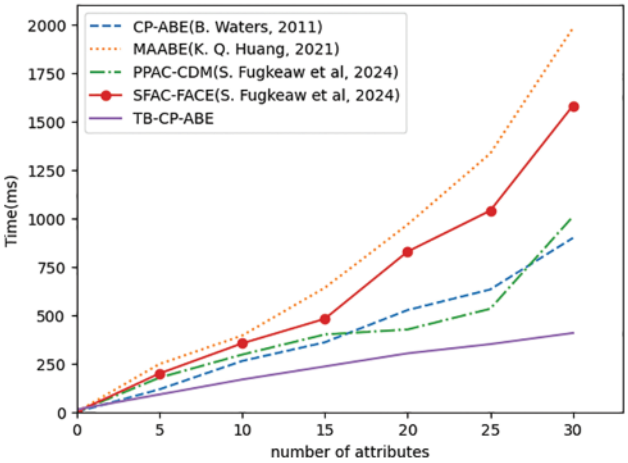

Figure 5: Performance of *ESDec* [22,25,27,28]

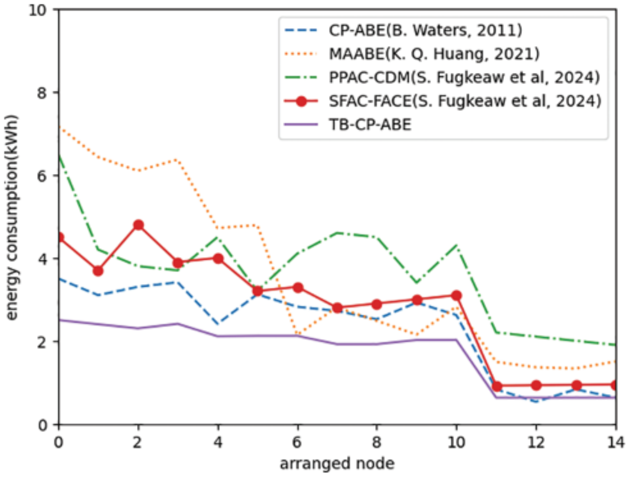

Figure 6: Energy demand comparison [22,25,27,28]

(3) Scalability: Scalability refers to how efficiently the dynamic access control mechanism handles the growth in network overhead or the time required to complete all necessary calculations as the number of DU nodes increases. Starting with an initial count of 10 nodes, the system's scalability is evaluated by incrementally adding five nodes at a time until 800 nodes, where each new set of nodes brings a proportional increase in computing power. In essence, scalability measures the ability of the access control system to adapt and maintain performance as the network expands.

Fig. 7 illustrates the variation in network computation time as the number of nodes expands. The proposed TB-CP-ABE exhibits a linear growth in computation time as the number of nodes increases, indicating a steady but predictable rise in processing requirements. In contrast, due to the poorly expressive access structure, References [27,28] have longer overall computation times as the number of devices increases, indicating that it may not be able to scale effectively. On the other hand, References [22,25] start with lower computation times. However, as the number of nodes increases, the complex scheme process introduces huge overhead, resulting in a rapid increase in computation time, highlighting the potential scalability challenges of this method under network growth conditions.

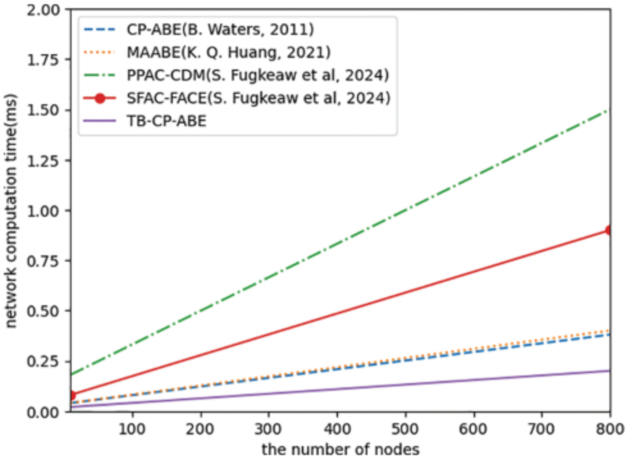

Figure 7: Scalability comparison [22,25,27,28]

(4) Latency Test: The purpose of latency testing is to examine the device's ability to process messages. The experiment will calculate the time taken by DU from initiating the request to receiving the ciphertext and decrypting it. The latency requirement for general real-time services is 50 ms. From Fig. 8, it can be seen that due to excessive bilinear operations and frequent message passing, the delays of [25,27,28] are relatively large (mostly above 50 ms), making them unsuitable for real-time network environments. The delay of the method is close to that of the proposed algorithm, but due to the early proposal of the scheme, the security cannot meet the current requirements.

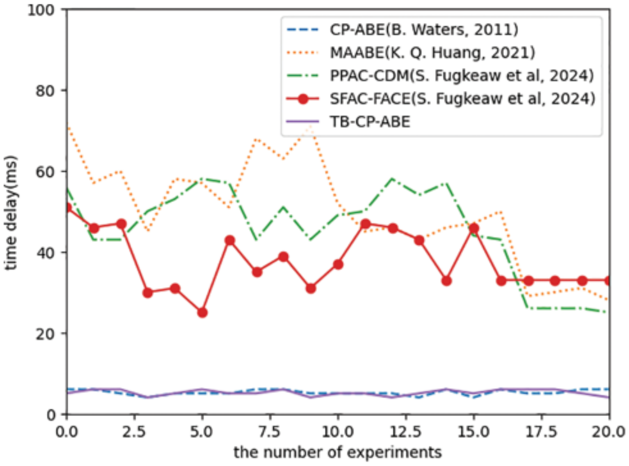

Figure 8: Time delay comparison [22,25,27,28]

7 Conclusion

In this article, a trust-based device access control CP-ABE scheme has been proposed for RES, which efficiently manages the distribution and control of encrypted data on the cloud through attribute key management. Due to the structural requirements of RES and the constraints of resource-limited terminals, the proposed scheme utilizes outsourced decryption to significantly mitigate the computational burden introduced by bilinear pairing operations. Moreover, the integration of attribute revocation and trust management enhances the flexibility and adaptability of the scheme in attribute and terminal management. A formal security analysis demonstrates that TB-CP-ABE scheme provides security against CPA. Analysis of performance demonstrates that TB-CP-ABE scheme optimizes the trade-off between computational and communication costs. This is particularly evident when comparing operational efficiency, message lengths, and security characteristics with other existing schemes, highlighting a notable reduction in the burden on resource-constrained terminals. In conclusion, the proposed TB-CP-ABE scheme offers a robust and efficient solution for securing RES, thereby advancing secure access control in cloud-assisted RES.

It is worth noting that while blockchain has shown great potential in ensuring data transaction security due to its decentralized, tamper-proof, and highly transparent characteristics, this paper has not yet considered this emerging technology when exploring device security transaction technologies. To further enhance data security and sharing efficiency, future research will focus on exploring the integration of blockchain with Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This approach aims to create a decentralized data security sharing environment, providing more reliable security guarantees and flexible access control mechanisms for data transactions. In addition, we plan to apply machine learning for dynamic trust evaluation and test this scheme in various cloud-based Renewable Energy Systems (RES) environments. Through these efforts, we aim to achieve smarter and more efficient data security management, further improving the adaptability and security of the system.

Acknowledgement: The authors express their sincere gratitude to all individuals who have contributed to this paper. Their dedication and insights have been invaluable in shaping the outcome of this work.

Funding Statement: This work was supported by the Science and Technology Project of the State Grid Corporation of China, Grant number 5700-202223189A-1-1-ZN.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Kehe Wu, Zheng Tian; data collection: Yizhen Sun, Yuxi Wu, Yaogong Guo; analysis and interpretation of results: Jiyu Zhang, Ruomeng Yan; draft manuscript preparation: Jiyu Zhang, Ruomeng Yan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author, Jiyu Zhang, upon reasonable request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] M. M. Alam, A. Haque, M. A. Khan, N. M. Sobahi, I. M. Mehedi and A. I. Khan, “Condition monitoring and maintenance management with grid-connected renewable energy systems,” *Comput. Mater. Contin.*, vol. 72, no. 2, pp. 3999–4017, 2022. doi: 10.32604/cmc.2022.026353.

[2] N. R. R. Paul and D. P. Raj, “Enhanced trust based access control for multi-cloud environment,” *Comput. Mater. Contin.*, vol. 69, no. 3, pp. 3079–3093, 2021. doi: 10.32604/cmc.2021.018993.

[3] H. A. Hussain, Z. Mansor, Z. Shukur, and U. Jafar, “Ether-IoT: A realtime lightweight and scalable blockchain-enabled cache algorithm for iot access control,” *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 3797–3815, 2023. doi: 10.32604/cmc.2023.034671.

[4] A. Sahai and B. R. Waters, “Fuzzy identity based encryption,” in *Proc. Eur. Cryptol. Conf.*, Aarhus, Denmark, 2005, pp. 457–473.

[5] L. H. Guo, J. Yang, and H. T. Wu, “A lightweight abe security protection scheme in cloud environment based on attribute weight,” *Comput. Mater. Contin.*, vol. 76, no. 2, pp. 1929–1946, 2023. doi: 10.32604/cmc.2023.039170.

[6] L. Nkenyereye, S. M. R. Islam, M. Hossain, M. Abdullah-Al-Wadud, and A. Alamri, “Fog-based secure framework for personal health records systems,” *Comput. Mater. Contin.*, vol. 66, no. 2, pp. 1937–1948, 2021. doi: 10.32604/cmc.2020.013025.

[7] K. P. Xue, N. Gai, J. N. Hong, D. S. L. Wei, P. L. Hong and N. H. Yu, “Efficient and secure attribute-based access control with identical sub-policies frequently used in cloud storage,” *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 635–646, 2022. doi: 10.1109/TDSC.2020.2987903.

[8] Z. S. Zhang, W. Huang, S. J. Zhou, and Y. J. Liao, “A revocable multi-authority fine-grained access control architecture against ciphertext rollback attack for mobile edge computing,” *J. Syst. Archit.*, vol. 129, no. 102589, p. 20, 2022. doi: 10.1016/j.sysarc.2022.102589.

[9] J. Zhao, P. Zeng, and K. K. R. Choo, “An efficient access control scheme with outsourcing and attribute revocation for fog-enabled e-health,” *IEEE Access*, vol. 9, pp. 13789–13799, 2021. doi: 10.1109/ACCESS.2021.3052247.

[10] S. M. Xu *et al.*, “Match in my way: Fine-grained bilateral access control for secure cloud-fog computing,” *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 1064–1077, 2022.

[11] C. Ge, Z. Liu, W. Susilo, L. Fang, and H. Wang, “Attribute-based encryption with reliable outsourced decryption in cloud computing using smart contract,” *IEEE Trans. Depend. Secure Comput.*, vol. 21, no. 2, pp. 937–948, 2023. doi: 10.1109/TDSC.2023.3265932.

[12] Q. Li, Q. Zhang, H. Huang, W. Zhang, W. Chen and H. Wang, “Secure, efficient, and weighted access control for cloud-assisted industrial IoT,” *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16917–16927, 2022. doi: 10.1109/JIOT.2022.3146197.

[13] L. Y. Zhang, W. T. You, and Y. Mu, “Secure outsourced attribute-based sharing framework for lightweight devices in smart health systems,” *IEEE Trans. Serv. Comput.*, vol. 15, no. 5, pp. 3019–3030, 2022. doi: 10.1109/TSC.2021.3073740.

[14] Y. Tao *et al.*, “ORR-CP-ABE: A secure and efficient outsourced attribute-based encryption scheme with decryption results reuse,” *Future Gener. Comput. Syst.*, vol. 161, pp. 559–571, 2024. doi: 10.1016/j.future.2024.07.040.

[15] R. H. Xu, J. Joshi, and P. Krishnamurthy, “An integrated privacy preserving attribute-based access control framework supporting secure deduplication,” *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 2, pp. 706–721, 2021. doi: 10.1109/TDSC.2019.2946073.

[16] H. Xiong, K. K. R. Choo, and A. V. Vasilakos, “Revocable identity-based access control for big data with verifiable outsourced computing,” *IEEE Trans. Big Data*, vol. 8, no. 1, pp. 1–13, 2022. doi: 10.1109/TBDATA.2017.2697448.

[17] H. Ma, R. Zhang, S. Z. Sun, Z. S. Song, and G. S. Tan, “Server-aided fine-grained access control mechanism with robust revocation in cloud computing,” *IEEE Trans. Serv. Comput.*, vol. 15, no. 1, pp. 164–173, 2022. doi: 10.1109/TSC.2019.2925028.

[18] W. J. Liu, W. Y. Chiu, and W. Hua, "Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach," *Energy*, vol. 290, 2024. doi: 10.1016/j.energy.2023.130110.

[19] L. Feng *et al.*, "SDAC-BBPP: A secure dynamic access control scheme with blockchain-based privacy protection for IIoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 3, pp. 3179–3193, 2024. doi: 10.1109/TNSM.2024.3371521.

[20] A. A. Alqbaishi and A. E. S. Ahmed, "Reputation evaluation using fuzzy logic for blockchain-based access control in an IoT environment," *IEEE Access*, vol. 12, pp. 97386–97404, 2024. doi: 10.1109/ACCESS.2024.3426993.

[21] Y. Wei, K. Gai, J. Yu, L. Zhu, and K. K. R. Choo, "Trustworthy access control for multiaccess edge computing in blockchain-assisted 6G systems," *IEEE Trans. Ind. Inform.*, vol. 20, no. 5, pp. 7732–7743, 2024. doi: 10.1109/TII.2024.3360467.

[22] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. 14th Int. Conf. Pract. Theor. Public Key Cryptogr.*, Taormina, Italy, 2011, pp. 53–70. doi: 10.1007/978-3-642-19379-8_4.

[23] K. Sethi, A. Pradhan, and P. Bera, "Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation," *J. Inf. Secur. Appl.*, vol. 51, 2020, Art. no. 102435. doi: 10.1016/j.jisa.2019.102435.

[24] Z. S. Zhang and S. J. Zhou, "A decentralized strongly secure attribute-based encryption and authentication scheme for distributed internet of mobile things," *Comput. Netw.*, vol. 201, 2021, Art. no. 108553. doi: 10.1016/j.comnet.2021.108553.

[25] K. Q. Huang, "Secure efficient revocable large universe multi-authority attribute-based encryption for cloud-aided IoT," *IEEE Access*, vol. 9, pp. 53576–53588, 2021. doi: 10.1109/ACCESS.2021.3070907.

[26] S. S. Tu, M. Waqas, F. M. Huang, G. Abbas, and Z. H. Abbas, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing," *Comput. Netw.*, vol. 195, 2021, Art. no. 108196. doi: 10.1016/j.comnet.2021.108196.

[27] S. Fugkeaw and L. Hak, "PPAC-CDW: A privacy-preserving access control scheme with fast OLAP query and efficient revocation for cloud data warehouse," *IEEE Access*, vol. 12, pp. 78743–78758, 2024. doi: 10.1109/ACCESS.2024.3408221.

[28] S. Fugkeaw, R. Prasad Gupta, and K. Worapaluk, "Secure and fine-grained access control with optimized revocation for outsourced IoT EHRs with adaptive load-sharing in fog-assisted cloud environment," *IEEE Access*, vol. 12, pp. 82753–82768, 2024. doi: 10.1109/ACCESS.2024.3412754.