sensors

MDPI

Article

Access Control Based on Ciphertext Attribute Authentication and Threshold Policy for the Internet of Things

Qikun Zhang [1], Yongjiao Li [1,*], Zhigang Li [1], Junling Yuan [1], Yong Gan [2] and Xiangyang Luo [3]

[1] School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China; zhangqikun04@163.com (Q.Z.); lizg.cn@hotmail.com (Z.L.); yuanjunling@foxmail.com (J.Y.)
[2] Zhengzhou Institute of Technology, Zhengzhou 450044, China; ganyong@zzuli.edu.cn
[3] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China; xiangyangluo@126.com
* Correspondence: Lyjiao01@163.com

Received: 28 October 2019; Accepted: 25 November 2019; Published: 28 November 2019

Abstract: The development of the Internet of Things has led to great development of data sharing and data interaction, which has made security and privacy more and more a concern for users. How to ensure the safe sharing of data, avoid the leakage of sensitive information, and protect the privacy of users is a serious challenge. Access control is an important issue to ensure the trust of the Internet of Things. This paper proposes an access control scheme based on ciphertext attribute authentication and threshold policy, which uses the identity authentication of hidden attributes and divides the user's permission grade by setting the threshold function with the user's attributes. Users obtain different permission grades according to attribute authentication and access data of different sensitivity grades to achieve fine-grained, flexible and secure access to data in the cloud server while protecting personal privacy issues. In addition, when the resource is acquired, the identity and permission joint authentication method is adopted to avoid the collusion attack of the illegal member, which makes the resource access control more secure.

Keywords: Internet of Things; attribute-based encryption; access control; data security sharing; attribute authentication

1. Introduction

The development of the Internet of Things has spawned the emergence of new informatization concepts such as smart homes, smart cities, and mobile crowd sensing. It connects people, people and things, things and things on the Internet, and realizes information exchange, collaborative operation, and resource sharing among terminal entities through wired or wireless network technologies according to different physical environments and application scenarios [1]. It is widely used in various fields of the information society, such as remote control of intelligent terminals for remote medical treatment, unmanned vehicle driving in the in-vehicle networks and intelligent sensor data, and remote physical environment monitoring in remote areas. The development of the Internet of Things has brought great convenience to people's lives, promoted the rise of the sharing economy, and promoted the development of society.

At the same time, the development of the Internet of Things is also facing some serious challenges: In the field of physical technology, with the improvement of people's living standards, people's application requirements for the Internet of Things are constantly improving, such as the real-time nature of Internet of Things communication, the bandwidth of the Internet of Things, and the energy

consumption of the Internet of Things. Different application scenarios will also involve specific requirements regarding scope, power consumption, throughput, and network topology. These are issues that the Internet of Things needs to further improve and solve [2]. In the field of information application, the popularization and application of the Internet of Things involves various fields of people's life and work. The vulnerability of the Internet of Things makes the communication information, identity information, and shared information among terminal entities easily exposed to the open Internet of Things. Securing the confidentiality of IoT communication information, the concealment of identity information, and the security of shared information are another challenge facing the Internet of Things. Therefore, it is necessary to develop the innovative information technology of the Internet of Things, the privacy protection of users, and the security of interactive data and shared data [3].

The powerful interoperability of the Internet of Things has accelerated the data aggregation and data sharing in the Internet of Things, making the Internet of Things one of the infrastructures in many fields such as medical and intelligent transportation. To protect data security in the Internet of Things, data are typically stored in encrypted form on the server, and attribute-based encryption has proven to be a powerful encryption tool. At the same time, it is crucial to propose effective access control policies to access these encrypted data and protect the security of some sensitive information. In recent years, research on access control of data has emerged in an endless stream attribute-based encryption strategies are widely used in medical, corporate, and personal areas. Privacy protection and field access for personal health information forms for medical use attribute-based encryption methods, and permission settings for access control [4], which can protect privacy and flexible access, bringing great benefits to the medical industry. A comprehensive study of some different access control models and access control architectures provides a future direction for IoT access control research [5]. Verifiable threshold multi-permission access control constructs a mixed multi-permission scheme [6]; on the basis of one permission maintaining the whole attribute set encryption scheme, unified attribute setting managed by multiple departments can guarantee the security of data.

With the rapid development of big data, security in the fields of information storage, information acquisition, and information transmission has become a serious problem. The powerful interoperability and flexible access features of the Internet of Things have greatly threatened data security and personal privacy. Aiming at these problems, this paper proposes an access control scheme based on ciphertext attribute authentication and threshold policy for the Internet of Things (AC-CAATP), which uploads the data to the cloud server after encrypting the data, and uses attributes to set a threshold policy to limit the user's access to the data. Similarly, the user authenticates the identity based on the attribute and obtains different permission grades from the certificate authority, and then accesses the data of the corresponding sensitivity grade. The protocol combines the advantages of attribute-based encryption technology and access control strategy to ensure data security and user privacy. At the same time, an access control policy is set for data access, which avoids the leakage of sensitive information.

1.1. Contributions

In this paper, an access control scheme based on ciphertext attribute authentication and threshold policy for the Internet of Things is proposed. The research contributions of this paper can be summarized as follows:

(1) Hidden attribute authentication: An identity authentication technology based on hidden attributes is proposed, which not only hides the user's identity information, but also hides the user's attribute information. In the process of identity authentication, the advantages of the traditional key agreement protocol identity authentication are preserved, and the attribute information is hidden by the algorithm to avoid revealing the user's personal privacy.
(2) Lightweight and efficient access control technology: Traditional attribute-based access control mostly adopts complex access control policies, such as tree-based access control policies,

which require a large number of intermediate nodes to calculate and transmit messages during data access, thus increasing a large amount of computational and communication overhead. In this paper, permission list query and threshold function are used to implement access control. A large number of nodes are not required to transmit information during the access process. Therefore, the computational amount is small and the computational time is short, which is more suitable for a mobile terminal device with limited resources and requiring fast resource access.

(3) High security: Traditional attribute-based access control is difficult for resisting collusion attacks. For example, when a user does not have enough attribute sets to access a resource, he can get enough attributes in conjunction with other users who do not have access to the resource to gain access to the resource. In this paper, the identity and permission joint authentication method is adopted in resource acquisition. When each user registers, the same attribute of different users obtains different permission parameters. Therefore, users cannot jointly access resources by using other members' attributes. At the same time, this paper also adopts permission authentication when accessing resources. Users who do not reach the access level cannot access and download ciphertext resources, making resource access more secure.

1.2. Organization

In Section 2, the related work of this paper is described; in Section 3, the basic knowledge is described; in Section 4, the details of AC-CAATP scheme are described; in Section 5, the correctness and security analysis of AC-CAATP is described, and we further analyze the efficiency of AC-CAATP in Section 6; the conclusions of the paper are in Section 7.

2. Related Work

While the Internet of Things is widely used, the vulnerability of its network is subject to severe security challenges. In recent years, IoT security has become a personal issue for scholars at home and abroad, especially IoT data security exchange, IoT intrusion detection, and IoT access control. Intrusion detection research based on the Internet of Things was proposed in [7–9]; three methods are proposed in the literature to detect intrusion events in the network, which can prevent and resolve malicious attacks and improve the security of IoT applications. An overview of secure communication among vehicles is presented in [10], which describes cases in which multiple connected entities interact with appropriate communication protocols, analyzing, researching, and evaluating the most relevant systems, applications, and communication protocols, further improving road safety and predicting the potential danger of road traffic. In [11], a data exchange scheme based on wireless devices in a physical Internet of Things is proposed. It is based on two core elements with interchangeable roles, entities and trackers, using a blockchain-based distributed paradigm, existing infrastructure, and equipment to ensure anonymization and immutability of the data involved. This section focuses on the introduction and analysis of research work related to IoT access control.

In this era of information explosion and network sharing, safeguarding data and information security is a serious challenge for us. Some access to sensitive information requires some permission. More and more scholars have analyzed and studied this situation. In [12], a novel attribute based access control scheme for IoT systems is proposed, which simplifies greatly the access management. It uses block-chain technology to record the distribution of attributes in order to avoid single point failure and data tampering. The access control process has also been optimized to meet the need for high efficiency and lightweight calculation for IoT devices. In [13], the authors comprehensively expound the existing access control mechanisms used in the cloud computing environment, analyze the advantages and disadvantages of these models and application requirements, and evaluate the existing access control mechanisms based on these requirements.

In [14,15], in view of the limitation of medical resources in the Internet of Things, an access control system is proposed. The system provides authorized users with fine-grained access to services while protecting valuable resources from unauthorized access. In addition, the application attribute assigns

a role to the member and authorizes the member to access the IoT device to provide a specific service. A secure and efficient multi-authority access control system for IoT-enabled mHealth is proposed in [16], there are multiple independent attribute authorities in the system, and a new entity can attribute authority without rebuilding the system. In addition, most of the decryption is performed in the cloud server, only returning part of the decrypted ciphertext, greatly reducing the user's decryption overhead.

In [17], a scalable enhanced key aggregation cryptosystem is proposed to implement security level management. This method uses the improved Diffie–Hellman key exchange algorithm (IDHKE) to achieve secure data sharing and key security sharing of data receivers. For security and consistent access control restrictions, attribute-based encryption is used to ensure the accuracy and reliability of protected data transmission. In [18,19], the medical big data security utilization encryption and access control process was analyzed. The classification method is used to classify and encrypt sensitive data and non-sensitive data in cloud computing, and triple DES (TDES) is encrypted and stored in the cloud, and a feasible optimization technique is proposed, Finally, the attribute-based access control authentication phase is used to authenticate the data in the cloud sim. The clustering, classification and encryption results of the method are compared with existing methods.

In order to protect the confidentiality of data and solve the problem of leaking data or leaking user keys for different reasons based on attribute conditions, an attribute-based batch cloud access control system is proposed in [20] that introduces an efficient, revocable, attribute-based encryption scheme that enables data owners to efficiently manage the credentials of data users. In [21], a new security and privacy-based Connected Vehicle Network Access Control (SPBAC) model is proposed, which allows security officials to access information through permissions and roles, rather than just accessing the same fleet of officials through roles. The model sets up multiple security layer maintenance, and each security layer coordinates and communicates with each other to avoid leakage of sensitive information.

A security solution based on RFID card-based physical biometric access control is proposed in [22]. This scheme combines RFID technology and dual watermark technology to provide a biometric control access framework. The wavelet packet decomposition watermark algorithm is used to insert fingerprint (detail) features. Into the face image of the authorized person, the same watermark algorithm is then used to insert the fingerprint watermark into the face feature extracted by the Gabor filter in the previously watermarked face image, and, finally, the obtained secure watermark biometric data are integrated into the RFID card, efficiently preventing information theft and illegal access to sensitive data. In [23], the paper analyzes the key indicators affecting the privacy disclosure of big data in health management, and establishes a risk-based access control model based on fuzzy theory for intelligent medical big data management, which solves the problem that the experimental results are inaccurate due to the lack of real data when the actual problem is processed. Protecting information security issues in smart medical management largely avoids patient privacy issues.

A security model based on IoT and fog cooperation is proposed in [24]. The model integrates an efficient access control process associated with the monitoring solution to ensure secure cooperation between different resources and different operational parts. Introduce a distributed access control based on the secure resource management framework for the fog-IoT network, and an active security scheme under super-trusted and low latency constraints. The solution not only has low latency, high security and confidentiality, but also reduces the management and management complexity of security and resource mechanisms. A distributed access control with outsourced encryption and decryption for electronic health records is introduced in [25]. The device combines the advantages of the fog device, which provides calculation, transmission, and storage services for the user, so the communication and calculation costs are lower. This scheme is a practical and novel solution.

In [26,27], in order to implement a secure service composition, a privacy-protected access control model and framework is proposed. In the model, an access request for a service is permitted if the requester's attribute certificates and contextual conditions are in compliance with the access control policies specified by the service provider and simultaneously the privacy preferences of the requester

are compatible with the privacy policies of the service provider. In the framework, the possible combined service chains are sorted according to the user's preference and the sensitivity of the data, and the security policy of the combined service is established by the selected service chain. A sensor platform for controlling an obstacle at the entrance of a vehicle is proposed in [28]. The platform enables automatic identification of the vehicle by image-based license plate recognition of the vehicle. First, an approaching vehicle is detected by an ultrasonic sensor, and, at the same time, an image is captured by a camera mounted on an obstacle, and then the license plate is automatically extracted from the image, and the license plate character is further divided. Finally, these characters are identified using standard optical character recognition (OCR) pipelines.

An access control system defined by blockchain technology is proposed in [29]. The system encodes the attribute-based access control policy into a smart contract and deploys it on the blockchain, thus transforming the policy evaluation process into a fully distributed intelligent contract execution, while the invariance and transparency of blockchain technology ensure the auditability of access control strategy evaluation. A new verifiable outsourcing ciphertext-policy attribute-based encryption scheme for big data privacy and access control in the cloud is proposed in [30,31], The solution reduces the computational overhead of encryption and decryption by outsourcing heavy computing to a proxy server, and verifies the correctness of the data through outsourced computation. In addition, the solution protects data security by limiting the data access of a group of users rather than providing unlimited data access.

In [32], cloud-based e-learning is implemented using an access control mechanism to prevent cloud resources from being accessed by unauthorized users. The system uses a key management scheme of access control technology to achieve secure content sharing and protection of the e-learning environment, and is more flexible and scalable in accessing e-learning content. A cloud computing data protection model is proposed in [33], which uses cryptography and access control to ensure the confidentiality, integrity, and proper control of sensitive data access. The model uses an enhanced RSA encryption algorithm combined with a role-based access control model and Extensible Access Control Markup Language (XACML) to improve security and allow data access. An edge-based encryption-based access control method (eri-ac) is proposed in [34]. This method encrypts the content using a symmetric key. The content key is secondarily encrypted by the producer and the edge router using edge re-encryption. Only authorized users can decrypt the re-encrypted content key with their private key to obtain the plaintext of the content. This method allows the user to obtain the content key from the producer, which can shorten the retrieval time and there is no copy redundancy.

In [35], the priority of the sensor is set according to the importance level of the sensor, the sampling rate, the timeout condition, and the remaining energy. Then, based on the priority of the node and the channel factor, a utility function is introduced to characterize the value of the node transmitting the data frame during a certain period of time. The time slot allocation problem is modeled. The goal is to maximize the total data transmission utility of all nodes in a specified time period by adjusting the transmission time and transmission duration of each node. According to the problem model, a time slot allocation scheme based on greedy strategy is proposed, which effectively reduces the time complexity of direct problem solving. In this scheme, nodes with higher priority are arranged to transmit data frames in time slots with better channel conditions. A transportation system boarding scheme for automatically controlling the number of passengers in the transport warehouse is proposed in [36]. The scheme uses the queuing theory to derive random numbers of passenger queue length, waiting time, and cabin capacity for determining the number of passengers arriving and the number of cabins arriving at Poisson. The expression of the nature deduces the cabin capacity and stability threshold of each station in the case of general passenger arrival distribution to control the number of passengers in the transport warehouse.

A crowdsourcing method for location-aware secure access (LaSa) control is proposed in [37], in which LaSa detects whether a user enters or leaves a room by discovering and identifying unique signal patterns. Combined with received signal strength (RSS), channel state information (CSI) and

coarse angle of arrival (AoA) data, the accuracy of wireless network user classification is improved. In [38], a model is designed and presented in this study in order to enable the privileged accounts to be controlled, managed, and followed at minimum cost. The model can set a strong password based on basic IT security principles and refine the scope of IT staff to reduce their workload, and improve managers' awareness of IT security to determine the password for a privileged user account. A function-based identity-based encryption-based IoT access control scheme is proposed in [39]. The program provides fine-grained access control to prevent applications from accessing unauthorized functions. At the same time, the cost of each access operation is a constant. In addition, the solution is secure, and prevents excessive privileged access.

At the same time, there are some studies on the analysis and evaluation of IoT security. A network and physical security vulnerability assessment based on the Internet of Things is proposed in [40], which outlines the application of the Internet of Things in the smart home sector, brings convenience and presents security and privacy challenges. Detect and identify possible security risks and vulnerabilities, fully understand the security status of smart homes, and propose ways to reduce risk. A survey of potential security issues with network protocols was proposed in [41]. The investigation raised the security and privacy issues in network protocols, analyzed vulnerabilities and security threats that are prone to networks, and agreed on new defense benchmarks.

It can be seen from the analysis of the above research results that the above research has a certain degree of deficiencies in terms of personal privacy protection, lightweight quality, and security. The rapid development of the Internet of Things has gradually changed people's way of life, flooding all aspects of life, and people's security requirements for the Internet of Things are getting higher and higher. According to the characteristics of the Internet of Things, such as limited mobile resources and easy disclosure of personal privacy, we propose an access control scheme based on ciphertext attribute authentication and threshold policy, in which further optimizations have been made in terms of personal privacy protection, lightweight and security. Through comparative analysis, the effect of this scheme is better.

3. Basic Knowledge and Security Assumptions

3.1. Bilinear Mapping

This paper is based on the basic theory of bilinear mapping; some basic knowledge related to bilinear mapping will be described in this section.

Let G_1 be an additive group and G_2 is a multiplicative group. Both of them have the same prime order q, where $q \geq 2^{\ell} + 1$, and ℓ is a security parameter. G_1 is generated by g_1 that means $G_1 = \langle g_1 \rangle$, and the discrete logarithm problems of G_1 and G_2 are difficult. We call e an admissible pairing, if $e : G_1 \times G_1 \to G_2$ satisfies the follow properties:

(1) Bilinear: For all $u, v \in G_1$, and $a, b \in \mathbb{Z}_q^*$, there is $e(au, bv) = e(u, v)^{ab}$;
(2) Non-degeneracy: There exists $u, v \in G_1$, such that $e(v, u) \neq 1$;
(3) Computability: For all $u, v \in G_1$, there exists a efficient way to calculate $e(v, u)$.

Inference 1. For all $u_1, u_2, v \in G_1$, there is $e(u_1 + u_2, v) = e(u_1, v)e(u_2, v)$.

3.2. Computational Complexity Problems

Definition 1. *Discrete Logarithm problem (DLP). Given an equation $Y = aP$, where $Y, P \in G_1$ and $a < q$. If a and P are given, it is easy to calculate Y. However, if P and Y are given, it will be difficult to calculate a.*

Definition 2. *Decisional Bilinear Diffie–Hellman (DBDH) Problem. Assume $G_1 = \langle g_1 \rangle$ is an additive group and $G_2 = \langle g_1, g_1 \rangle$ is a multiplicative group, Both of the two groups have the same large prime order q, where $q \geq 2^{\ell} + 1$, and ℓ is a security parameter, g_1 is the generator of group G_1. G_1 and G_2 is a pair of bilinear group, and $e : G_1 \times G_1 \to G_2$ is a calculable bilinear mapping. The following two triples $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$*

and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$*, for any* $a, b, c \in \mathbb{Z}_q^*$*,* $g_1 \in G_1$*,* $g_2 \in G_2$ *and* $\pi \in G_2$ *are computationally indistinguishable.*

$KeyGen(1^\lambda) \rightarrow (sk, pk)$: It takes as inputs the security parameter λ, and outputs a public/private key pair (sk, pk).

4. The Proposed Access Control Scheme

4.1. System Model

The system model we designed is shown in Figure 1, which consists of four entities: a certificate authority (CA), many data sharer, many data acquires, and a cloud server (CS). In addition, a user can be either a data acquirer or a data sharer.

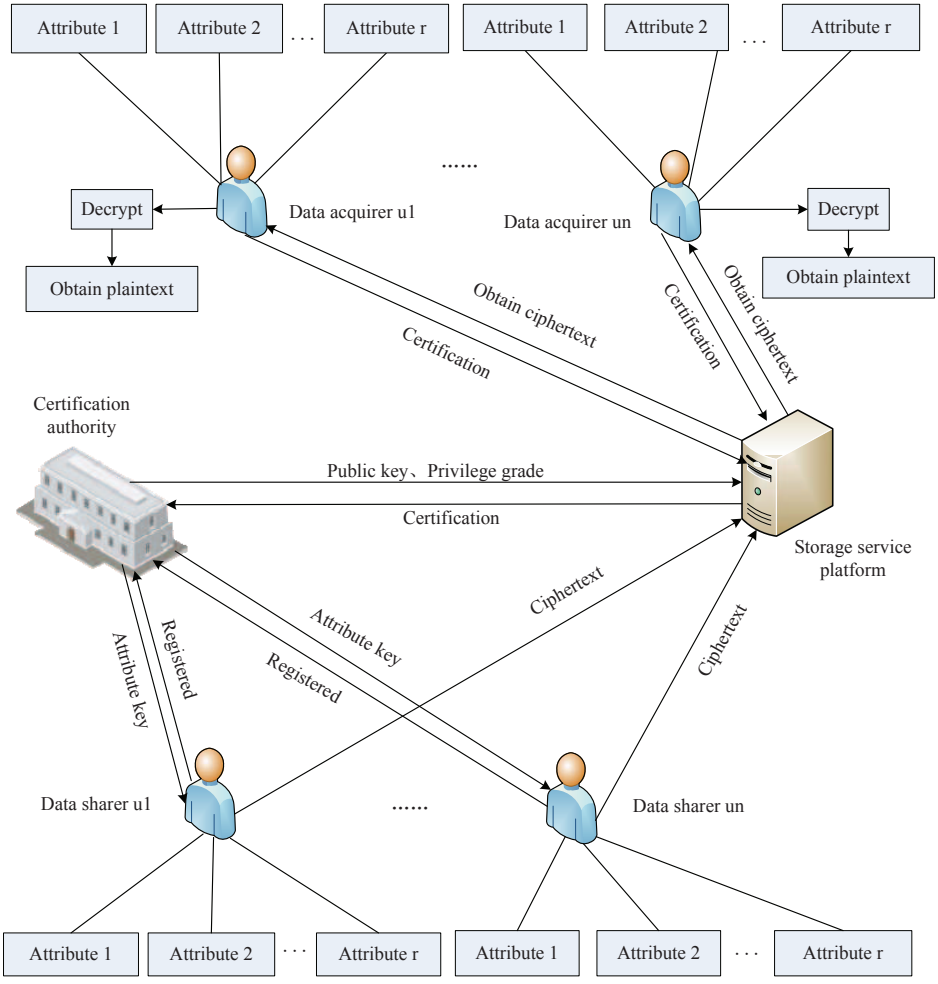

Figure 1. System model diagram.

The certificate authority (CA) is equivalent to the administrator of the system, who sets system parameters for access control and distributes secret key and privilege level information for the user.

The data sharer uploads his or her own data to the cloud server to share the data with other users. The data content is encrypted before being uploaded to the cloud server.

The data acquirer is an entity that is interested in the data stored in the cloud server, and can view and download related data in the cloud server according to its own access rights.

The cloud server (CS) is a public storage platform that provides data sharers with storage and shared encrypted data. Data requesters can freely access and download data stored in the cloud server according to their own permissions.

4.2. Initialization

In this section, we initialize an access control scheme based on ciphertext attribute authentication and threshold policy for Internet of Things. This access control system consists of a certification authority (CA), a cloud server (CS), and network terminal users. CA is a trusted entity used primarily for identity authentication, user registration, and attribute key distribution, and it also generates system public parameters and master keys. CS is an important entity, mainly used for the division of access rights of user encrypted information and the classification and storage of different access rights information. The system model is shown in Figure 1.

In this work, it is supposed that the protocol has n network terminals. Let $U = \{u_1, u_2, ..., u_n\}$ be the set of network terminals. In addition, the corresponding identity set is $ID = \{id_{u_1}, id_{u_2}, ..., id_{u_n}\}$. CA defines an ordered network attribute set $Attr = \{A_1, A_2, ..., A_j, ..., A_R\}$, where $A_j < A_{j+1}(j < R)$ and $R \in N^*$ denotes the number of the network attribute. In addition, $attr_i = \{a_{i,1}, a_{i,2}, ..., a_{i,r}\}$ is the ordered attribute set of network terminal u_i, where $attr_i \subseteq Attr$, $r \in N^*$, $r \leq R$ and $a_{i,r-1} < a_{i,r}$. i denotes the ith terminal and r denotes the rth attribute of u_i.

If the network terminal wants to store encrypted information on the cloud server or access encrypted information on the cloud server, it must register the attributes in the authentication center and obtain corresponding data storage and data access rights.

Assuming G_1 is an additive group, and the G_2 is a multiplicative group, they have the same large prime number order q, and discrete logarithm over G_1 and G_2 are difficult, $g_1 \in G_1$ is a generator of G_1. Parameter $e : G_1 \times G_1 \to G_2$ is a computable bilinear mapping. $H_1 : \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2 : G_1 \to \mathbb{Z}_q^*$ and $H_3 : G_2 \to \mathbb{Z}_q^*$ are three hash functions.

The CA runs the $KeyGen(1^\lambda)$ algorithm to obtain a public/private key pair (SK_A, PK_A), where $SK_A \in \mathbb{Z}_q^*$ and $PK_A = SK_A g_1$. The any member $u_i \in U(1 \leq i \leq n)$ chooses a random positive integer $s_{u_i} \in \mathbb{Z}_q^*$ and calculates $sk_{u_i} = H_1(id_{u_i})s_{u_i}$. sk_{u_i} as its private key and the public key $pk_{u_i} = g_1 sk_{u_i}$. The system parameters are $params = (PK_A, q, G_1, G_2, g_1, e, H_1, H_2, H_3)$.

4.3. Terminal Users Registration

The terminal users registration of AC-CAATP is depicted in Table 1, and the detailed steps are performed as follows:

(1) CA constructs an R degree polynomial(1) by using the elements in the network attribute set $Attr = \{A_1, A_2, ..., A_j, ..., A_R\}$ (arranged according to the sequence of attributes specified by the network system) as the coefficients of the polynomial:

$$f(x) = (x - A_R)(x - A_{R-1})...(x - A_1) = b_R x^R + b_{R-1} x^{R-1} + ... + b_0. \quad (1)$$

(2) Each terminal user $u_i(1 \leq i \leq n)$ with the attribute set $attr_i = \{a_{i,1}, a_{i,2}, ..., a_{i,r}\}$ (arranged according to the sequence of attributes specified by the network system) selects a random number $\lambda_i \in \mathbb{Z}_q^*(\lambda_i \neq 1, 0)$ and calculates $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ..., (\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1)\}$ and $\beta_i = (a_{i,1} + a_{i,2} + ... + a_{i,r}) sk_{u_i} \lambda_i g_1$. Then, u_i sends $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ..., (\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}$ to CA.

(3) After receiving the messages $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ..., (\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}$, CA calculates $\gamma_i = a_{i,1}\lambda_i g_1 + a_{i,2}\lambda_i g_1 + ... + a_{i,r}\lambda_i g_1$ and verifies the identity

of u_i by equation $e(\beta_i, g_1) = e(\gamma_i, pk_{u_i})$. If it holds, CA calculates the following formula (2) according to the ploynomial(1):

$$\begin{aligned} &b_0\lambda_i g_1 + b_1 a_{i,1}\lambda_i g_1 + ... + b_R a_{i,1}^R \lambda_i g_1 = f(a_{i,1})\lambda_i g_1, \\ &b_0\lambda_i g_1 + b_1 a_{i,2}\lambda_i g_1 + ... + b_R a_{i,2}^R \lambda_i g_1 = f(a_{i,2})\lambda_i g_1, \\ &... \\ &b_0\lambda_i g_1 + b_1 a_{i,r}\lambda_i g_1 + ... + b_R a_{i,r}^R \lambda_i g_1 = f(a_{i,r})\lambda_i g_1. \end{aligned} \tag{2}$$

If Equation (2) is equal to 0, this means that $f(a_{i,1}) = 0, f(a_{i,2}) = 0, ..., f(a_{i,r}) = 0$ and $attr_i \subseteq Attr$. Then, CA computes $Q_j = A_j\lambda_i g_1 (1 \leq j \leq R)$ and compares whether the equation $A_j\lambda_i g_1 = a_{i,\iota}\lambda_i g_1 (1 \leq \iota \leq r)$ is true. If it holds, CA can determine which attributes the user u_i has; according to the corresponding attribute values, CA selects the corresponding attribute parameters $t_{i,1}, t_{i,2}, ..., t_{i,r} \in \mathbb{Z}_q^*$. It calculates formula (3), and CA divides the permission level according to the number of their attributes and calculates formula (4) as the privilege grade:

$$\{T_{i,0} = \lambda_i g_1, T_{i,1} = t_{i,1}T_{i,0}, T_{i,2} = t_{i,2}T_{i,0}, ...T_{i,r} = t_{i,r}T_{i,0}\}, \tag{3}$$

$$\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + ... + t_{i,r})g_1. \tag{4}$$

Then, CA sends $\{\eta_{i,h}, T_{i,1}, T_{i,2}, ..., T_{i,r}\}$ to the register terminal u_i and secretly saves parameter γ_i. (Note that, for any two attributes $a_{i,k}$ and $a_{j,l}$ of different members of u_i and $u_j (i \neq j)$, if $a_{i,k} = a_{j,l}$, then $t_{i,k} = t_{j,l}$).

(4) After receiving the messages $\{\eta_{i,h}, T_{i,1}, T_{i,2}, ..., T_{i,r}\}$ from CA, $u_i (1 \leq i \leq n)$ calculates formula (5) and verifies the identity of CA by equation $e(\eta_{i,h}, g_1) = e(\varepsilon_i, PK_A)$. If it holds, u_i computes the following formula (6) according to formula (3) and obtains the attribute permission values $\{K_{i,1}, K_{i,2}, ..., K_{i,r}\}$ and the privilege level $\eta_{i,h}$:

$$\varepsilon_i = \lambda_i^{-1}T_i + \lambda_i^{-1}T_{i,2} + ... + \lambda_i^{-1}T_{i,r} = (t_{i,1} + t_{i,2} + ... + t_{i,r})g_1, \tag{5}$$

$$K_{i,1} = \lambda_i^{-1}T_{i,1} = t_{i,1}g_1, K_{i,2} = \lambda_i^{-1}T_{i,2} = t_{i,2}g_1, ..., K_{i,r} = \lambda_i^{-1}T_{i,r} = t_{i,r}g_1. \tag{6}$$

u_i sends messages $\{u_i, pk_{u_i}, \eta_{i,h}\}$ to CA indicating that it has successfully registered.

(5) After receiving the messages $\{u_i, pk_{u_i}, \eta_{i,h}\}$ from u_i, CA verifies the messages and sends it to CS.

With the above steps, all the terminals $u_i (1 \leq i \leq n)$ register successfully. In addition, CA can obtain the attribute information from all the registration terminals $u_i (1 \leq i \leq n)$. CA divides the permission levels of group members according to the number of attributes. Then, CA can build a terminal users registration information table (as shown in Table 2) and share the information resource with CS, which is used for querying user rights and access control of resource permissions.

Table 1. The terminal users registration process of ABE-AC.

Terminal Users	**CA**
$u_i(1 \le i \le n)$ The attribute set ofu_i: $attr_i = \{a_{i,1}, a_{i,2}, ..., a_{i,r}\}$	The attribute set of network : $Attr = \{A_1, A_2, ..., A_j, ..., A_R\}$ Construct polynomial function : $f(x) = b_R x^R + b_{R-1} x^{R-1} + ... + b_0$
Selects a random number : $\lambda_i \in \mathbb{Z}_q^*(\lambda_i \ne 1, 0)$ Calculates : $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1)$, $(\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1)$, $(\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1)\}$ $\beta_i = (a_{i,1} + a_{i,2} + ... + a_{i,r}) sk_{u_i} \lambda_i g_1$ $\xrightarrow{\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ..., (\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}}$	Calculates : $\gamma_i = a_{i,1}\lambda_i g_1 + a_{i,2}\lambda_i g_1 + ... + a_{i,r}\lambda_i g_1$ Verifies the equation :$e(\beta_i, g_1) = e(\gamma_i, pk_{u_i})$ Calculates : $b_0\lambda_i g_1 + b_1 a_{i,1}\lambda_i g_1 + ... + b_R a_{i,1}^R \lambda_i g_1 = f(a_{i,1})\lambda_i g_1$ $b_0\lambda_i g_1 + b_1 a_{i,2}\lambda_i g_1 + ... + b_R a_{i,2}^R \lambda_i g_1 = f(a_{i,2})\lambda_i g_1, ...,$ $b_0\lambda_i g_1 + b_1 a_{i,r}\lambda_i g_1 + ... + b_R a_{i,r}^R \lambda_i g_1 = f(a_{i,r})\lambda_i g_1$ Computes $Q_j = A_j \lambda_i g_1 (1 \le j \le R)$ Compares $A_j \lambda_i g_1 = a_{i,\iota}\lambda_i g_1 (1 \le \iota \le r)$ Chooses $t_{i,1}, t_{i,2}, ..., t_{i,r} \in \mathbb{Z}_q^*$ Calculates : $\{T_{i,0} = \lambda_i g_1, T_{i,1} = t_{i,1} T_{i,0}, T_{i,2} = t_{i,2} T_{i,0}, ...$ $T_{i,r} = t_{i,r} T_{i,0}\}$ $\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + ... + t_{i,r}) g_1$ $\xleftarrow{\{\eta_{i,h}, T_{i,1}, T_{i,2}, ..., T_{i,r}\}}$
Calculates : $\varepsilon_i = (t_{i,1} + t_{i,2} + ... + t_{i,r}) g_1$ Verifies the identity of CA : $e(\eta_{i,h}, g_1) = e(\varepsilon_i, PK_A)$ Calculates : $K_{i,1} = \lambda_i^{-1} T_{i,1} = t_{i,1} g_1,$ $K_{i,2} = \lambda_i^{-1} T_{i,2} = t_{i,2} g_1, ...,$ $K_{i,r} = \lambda_i^{-1} T_{i,r} = t_{i,r} g_1$ Obtains : $\{K_{i,1}, K_{i,2}, ..., K_{i,r}, \eta_{i,h}\}$ $\xrightarrow{\{u_i, pk_{u_i}, \eta_{i,h}\}}$	$u_i(1 \le i \le n)$register successfully

Table 2. The registration information of terminal users.

Terminals	u_1	u_2	...	u_n
Effectiveness	yes	yes	...	yes
Publickey	pk_{u_1}	pk_{u_2}	...	pk_{u_n}
Keywords	$keywords_1$	$keywords_2$	...	$keywords_n$
Description	D_1	D_2	...	D_n
Encryptionkey	PK_{g-u_1}	PK_{g-u_2}	...	PK_{g-u_n}
Ciphertext resource	c_1	c_2	...	c_n
Privilege grade	$\eta_{1,h}$	$\eta_{2,h}$	...	$\eta_{n,h}$
right parameter	$T_{i,1}$,...	$T_{2,1}$,...	...	$T_{n,1}$,...
Thresholdvalue	$y_{1,1}$,...	$y_{2,1}$,...	...	$y_{n,1}$,...

4.4. Resource Encryption Storage

Each terminal user can encrypt their shared resources and upload them to the cloud server. Any member $u_j(1 \leq j \leq n)$ with the attribute set $attr_j = \{a_{j,1}, a_{j,2}, ..., a_{j,r}\}$ and the privilege value $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + ... + t_{j,r})g_1$ in the network wants to share resources to the members who have the same or higher privileges than him. He can do the following steps to encrypt resources and upload them to the cloud server:

(1) u_j gets the information $T_{j,1}, ..., T_{j,r}$ from the information in Table 1 and computes formula (7) and formula (8):

$$T_{pub,j} = T_{j,0} = \lambda_j g_1, \tag{7}$$

$$T_{pri} = \sum_{\tau=1}^{r} T_{j,\tau} = \sum_{\tau=1}^{r} t_{j,\tau}\lambda_j g_1 = (t_{j,1} + ... + t_{j,r})\lambda_j g_1. \tag{8}$$

(2) u_j selects $m_j \in \mathbb{Z}_p^*$ randomly, then calculate formulas (9), (10), and (11), according to formulas (6), (7), and (8) and constructs a $(r-1)-th$ degree polynomial(12) according to the attribute permission values $\{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$ that it kept before and $f(0) = M_j$; then, it computes formula (13) according to formula (11) and $\varphi_j = sk_{u_j}(y_{j,1} + y_{j,2} + ... + y_{j,r})$. u_j uses $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ as encryption key and $SK_{g-u_j} = M_j$ as decryption key:

$$p_{u_j} = m_j T_{j,0} = m_j \lambda_j g_1, \tag{9}$$

$$M_j = m_j T_{pri}, \tag{10}$$

$$w_{j,1} = H_2(K_{j,1}), w_{j,2} = H_2(K_{j,2}), ..., w_{j,r} = H_2(K_{j,r}), \tag{11}$$

$$f(x) = m_j K_{j,r-1} x^{r-1} + ... + m_j K_{j,1} x + M_j, \tag{12}$$

$$f(w_{j,1}) = y_{j,1}, f(w_{j,2}) = y_{j,2}, ..., f(w_{j,r}) = y_{j,r}. \tag{13}$$

(3) u_j encrypts its shared resources information $m \in \mathcal{M}^*$ ($\mathcal{M}^*$: plaintext space) with encryption key $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$, which is that u_j chooses a random number $\varsigma_j \in \mathbb{Z}_p^*$, and calculates formulas (14), (15), and (16) according to formulas (4) and (9), the corresponding ciphertext information is $c_j = (v_j, V_j)$:

$$H_3(e(p_{u_j}, \eta_{j,h}))^{\varsigma_j}, \tag{14}$$

$$v_j = \varsigma_j PK_A, \tag{15}$$

$$V_j = m \oplus H_3((e(p_{u_j}, \eta_{j,h})^{\varsigma_j}). \tag{16}$$

Then, u_j uploads the shared ciphertext information $c_j = (v_j, V_j)$. The plaintext information of the keywords of the shared resource and the related description of the resource (search for related resources primarily for resource visitors), encryption key $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ and related calculation parameters $\{(y_{j,1}, y_{j,2}, ..., y_{j,r}), (T_{j,1}, T_{j,2}, ..., T_{j,r}), \varphi_j, pk_{u_i}, \eta_{j,h}\}$ to the CS. CS verifies the

identity of u_j by the equation $e((y_{j,1} + y_{j,2} + ... + y_{j,r}), pk_{u_i}) = e(\varphi_j, g_1)$. If it holds, CS publishes the information $\{u_j, pk_{u_j}, Keywords_j, D_j, PK_{g-u_j}, c_j, \eta_{i,h}, (y_{j,1}, y_{j,2}, ..., y_{j,r})\}$ on the public display platform as shown in Table 2, where $Keywords_j$ is the keywords of the shared resource, and D_j is the related description of the resource.

4.5. Resource Access and Sharing

(1) Each user $u_i (1 \leq i \leq n, i \neq j)$ in the cloud system wants to access resources in the system; it can search for the corresponding ciphertext resource according to the keyword and related content description and can view the provider of the resource and access rights that should be available to access the resource.

(2) If u_i wants to access certain resources and has the access rights of the resource, u_i computes formula (17) according to formula (5), and sends the messages $(pk_{u_i}, \eta_{i,h}, \sigma_i)$ to CS:

$$\sigma_i = sk_{u_i}\varepsilon_i. \tag{17}$$

Then, CS verifies the identity of u_i by the equation $e(\eta_{i,h}, pk_{u_i}) = e(\sigma_i, PK_A)$. If it holds, CS opens the corresponding resource link.

(3) u_i downloads the corresponding ciphertext resource $c_j = (v_j, V_j)$ from the CS. It can compute the corresponding attribute permission values $\{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$ according to the right parameters $(T_{j,1}, T_{j,2}..., T_{j,r})$ and corresponding threshold value $(y_{j,1}, y_{j,2}, ..., y_{j,r})$. It computes $w_{i,1} = H_2(K_{i,1}), w_{i,2} = H_2(K_{i,2}), ..., w_{i,r} = H_2(K_{i,r})$. u_i constructs polynomial (18) according to the information $\{(w_{i,1}, y_{j,1}), (w_{i,2}, y_{j,2}), ..., (w_{i,r}, y_{j,r})\}$ and Lagrange theorem:

$$f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \leq \omega \leq r, \omega \neq \chi} \frac{x - w_{i,\omega}}{w_{i,\chi} - w_{i,\omega}} \right) y_{j,\chi}. \tag{18}$$

In addition, it computes the constant term $M_i = f(0) = \sum_{\chi=1}^{r} \left(\prod_{1 \leq \omega \leq r, \omega \neq \chi} \frac{-w_{i,\omega}}{w_{i,\chi} - w_{i,\omega}} \right) y_{j,\chi} = M_j$ as its decryption key. u_i can also obtain the encryption key $PK_{g-u_k} = (p_{u_k}, \eta_{k,h}) = (p_{u_j}, \eta_{j,h})$ from Table 2.

(4) Anyone $u_i (1 \leq i \leq n, i \neq j)$ in the network system can calculate $m = V_j \oplus H_3(e(v_j, M_i))$ from ciphertext $c_j = (v_j, V_j)$, with a valid decryption key M_i.

5. Correctness and Security Analysis

This section mainly discusses some of the performances of AC-CAATP protocol. First, it proves the correctness of AC-CAATP protocol, then discusses the security of AC-CAATP protocol, and finally analyzes the performance of AC-CAATP protocol.

5.1. Correctness

The proof of the correctness of AC-CAATP protocol is in the following theorems.

Theorem 1. *Any legal user $u_i (1 \leq i \leq n)$ in the system can download the ciphertext resource corresponding to the access rights. This means if $\eta_{i,h} > \eta_{j,h}$, $u_i (1 \leq i \leq n)$ can download the ciphertext resource c_j.*

Proof. We assume that u_i has a set of attributes $attr_i = \{a_{i,1}, a_{i,2}, ..., a_{i,r}\}$ and the correspond attribute weight parameter is $\varepsilon_i = (t_{i,1} + t_{i,2} + ... + t_{i,r})g_1$. u_i declares that it has access hierarchical $\eta_{i,h}$. It signs the parameter ε_i and the signed message is $\sigma_i = sk_{u_i}\varepsilon_i$. Then, it sends the messages $(pk_{u_i}, \eta_{i,h}, \sigma_i)$ to CS. According to the protocol AC-CAATP, CS verifies the identity of u_i by the equation $e(\eta_{i,h}, pk_{u_i}) = e(\sigma_i, PK_A)$. If it holds, CS opens the corresponding resource link. Since $\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + ... + t_{i,r})g_1$ and $\sigma_i = sk_{u_i}\varepsilon_i$, according to the characteristics of bilinear mapping, there are

$e(\eta_{i,h}, pk_{u_i})$,
$= e(SK_A(t_{i,1} + t_{i,2} + ... + t_{i,r})g_1, sk_{u_i}g_1)$
$= e((t_{i,1} + t_{i,2} + ... + t_{i,r})g_1, g_1)^{SK_A sk_{u_i}}$
$= e(sk_{u_i}(t_{i,1} + t_{i,2} + ... + t_{i,r})g_1, SK_A g_1)$
$= e(\sigma_i, PK_A)$.

The attribute weight parameter $\varepsilon_i = (t_{i,1} + t_{i,2} + ... + t_{i,r})g_1$ is signed by u_i and CS. This means that CS can ensure u_i has the access hierarchical $\eta_{i,h}$. Then, CS opens the corresponding resource link c_j for u_i. u_i can download the ciphertext resource c_j.

□

Theorem 2. *Any member $u_i(1 \le i \le n)$ with access right $\eta_{i,h}$, if $\eta_{i,h} \ge \eta_{j,h}$, u_i can access the corresponding resources $m \in \mathcal{M}^*$ belonging to $u_j(1 \le j \le n, i \ne j)$. This means that member $u_i(1 \le i \le n)$ can decrypt the ciphertext information c_j that was encrypted by member $u_j(1 \le j \le n, i \ne j)$ using the encryption key $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$.*

Proof. If u_i has the access right $\eta_{i,h}$ and $\eta_{i,h} \ge \eta_{j,h}$, then u_i has the attribute permission values $K_{i,1} = t_{i,1}g_1 = K_{j,1}, K_{i,2} = t_{i,2}g_1 = K_{j,2}, ..., K_{i,r} = t_{i,r}g_1 = K_{j,r}$, It can compute $w_{i,1} = H_2(K_{i,1}), w_{i,2} = H_2(K_{i,2}), ..., w_{i,r} = H_2(K_{i,r})$. u_i can construct a polynomial $f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \omega \le r, \omega \ne \chi} \frac{x - w_{i,\omega}}{w_{i,\chi} - w_{i,\omega}} \right) y_{j,\chi}$ according to the information $\{(w_{i,1}, y_{j,1}), (w_{i,2}, y_{j,2}), ..., (w_{i,r}, y_{j,r})\}$ from registration information table and the Lagrange theorem, and compute the constant term $M_i = f(0) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \omega \le r, \omega \ne \chi} \frac{-w_{i,\omega}}{w_{i,\chi} - w_{i,\omega}} \right) y_{j,\chi} = M_j$ as its the decryption key.

Since $T_{pub,j} = T_{j,0} = \lambda_j g_1$, $T_{pri} = (t_{j,1} + ... + t_{j,r})\lambda_j g_1$, $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + ... + t_{j,r})g_1$, $p_{u_j} = m_j \lambda_j g_1$, $M_j = m_j T_{pri}$ and the ciphertext information is $c_j = (v_j, V_j)$, where $v_j = \varsigma_j PK_A$ and $V_j = m \oplus H_3((e(p_{u_j}, \eta_{j,h})^{\varsigma_j})$. Then, u_i uses its own solved key $M_i = M_i = m_j T_{pri}$ to do the following calculation:

$V_j \oplus H_3(e(v_j, M_i))$
$= m \oplus H_3(e(p_{u_j}, \eta_{j,h})^{\varsigma_j}) \oplus H_3(e(v_j, M_i))$
$= m \oplus H_3(e(m_j \lambda_j g_1, SK_A(t_{j,1} + t_{j,2} + ... + t_{j,r})g_1)^{\varsigma_j}) \oplus H_3(e(\varsigma_j PK_A, m_j T_{pri}))$
$= m \oplus H_3(e(m_j g_1, (t_{j,1} + t_{j,2} + ... + t_{j,r})PK_A)^{\lambda_j \varsigma_j}) \oplus H_3(e(\varsigma_j PK_A, m_j T_{pri}))$
$= m \oplus H_3(e(m_j g_1, (t_{j,1} + t_{j,2} + ... + t_{j,r})PK_A)^{\lambda_j \varsigma_j}) \oplus H_3(e(PK_A, m_j T_{pri})^{\varsigma_j})$
$= m \oplus H_3(e(m_j g_1, (t_{j,1} + t_{j,2} + ... + t_{j,r})PK_A)^{\lambda_j \varsigma_j}) \oplus H_3(e(PK_A, m_j(t_{j,1} + ... + t_{j,r})\lambda_j g_1)^{\varsigma_j})$
$= m \oplus H_3(e(m_j g_1, PK_A)^{(t_{j,1} + t_{j,2} + ... + t_{j,r})\lambda_j \varsigma_j}) \oplus H_3(e(PK_A, m_j g_1)^{(t_{j,1} + ... + t_{j,r})\lambda_j \varsigma_j})$
$= m$.

Thus, u_i can decrypt the ciphertext information c_j and get the corresponding plaintext resources m. □

5.2. Security Analysis

Theorem 3. *Users with low access rights cannot access resources with higher permission grades than themselves. This means $u_i(1 \le i \le n)$ with access right $\eta_{i,h}$, if $\eta_{i,h} < \eta_{j,h}$, u_i cannot get decryption key M_j by solving polynomial functions to decrypt the ciphertext information c_j and get the corresponding plaintext resources m.*

Proof. If $\eta_{i,h} < \eta_{j,h}$, this means that u_i does not have enough attribute permission values $K_{j,1} = t_{j,1}g_1, K_{j,2} = t_{j,2}g_1, ..., K_{j,r} = t_{j,r}g_1$. It cannot compute $w_{j,1} = H_2(K_{j,1}), w_{j,2} = H_2(K_{j,2}), ..., w_{j,r} = H_2(K_{j,r})$ to get the point pair $\{(w_{j,1}, y_{j,1}), (w_{j,2}, y_{j,2}), ..., (w_{j,r}, y_{j,r})\}$ and construct a polynomial $f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \omega \le r, \omega \ne \chi} \frac{x - w_{j,\omega}}{w_{j,\chi} - w_{j,\omega}} \right) y_{j,\chi}$.

□

Lemma 1. *If $w_{j,1}, w_{j,2}, ..., w_{j,r}$ are different numbers in the number field F, $y_{j,1}, y_{j,2}, ..., y_{j,r}$ are any set of numbers in the number field F. There is a unique polynomial $f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \omega \le r, \omega \ne \chi} \frac{x - w_{j,\omega}}{w_{j,\chi} - w_{j,\omega}} \right) y_{j,\chi}$ in which the degree is no greater than $r-1$, such that $f(w_{j,\tau}) = y_{j,\tau}$, where $\tau = 1, 2, ..., r$.*

Proof. Assume there are two polynomials $f(x)$ and $g(x)$ in $F(x)$, their degrees no greater than $r-1$, and they all satisfy the equations: $f(w_{j,\tau}) = y_{j,\tau}$, $g(w_{j,\tau}) = y_{j,\tau}$, where $\tau = 1, 2, ..., r$. □

Let $\partial(x) = f(x) - g(x)$, if $f(x) \ne g(x)$, then $\partial(x) \ne 0$. $\partial(x)$ is a polynomial with a degree no greater than $r-1$ and the polynomial has r solutions, which is impossible. Thus, $\partial(x) = 0$, which means that $f(x) = g(x)$, and polynomial $f(x)$ is unique.

Lemma 2. *Polynomial $f(x)$ has a unique solution.*

Proof. Assume $f(x) = c_{r-1}x^{r-1} + c_{r-2}x^{r-2} + ... + c_0$, for $f(w_{j,\tau}) = y_{j,\tau} (1 \le \tau \le r)$, there are

$$\begin{cases} c_0 + c_1 w_{j,1}^1 + c_2 w_{j,1}^2 + ... + c_{r-1} w_{j,1}^{r-1} = y_{j,1} \\ c_0 + c_1 w_{j,2}^1 + c_2 w_{j,2}^2 + ... + c_{r-1} w_{j,2}^{r-1} = y_{j,2} \\ ..... \\ c_0 + c_1 w_{j,r}^1 + c_2 w_{j,r}^2 + ... + c_{r-1} w_{j,r}^{r-1} = y_{j,r}. \end{cases}$$

This is a linear system of equations with unknown numbers $c_0, c_1 .... c_r$. Its coefficient determinant is as follows:

$$|A| = \begin{vmatrix} 1 & w_{j,1}^1 & w_{j,1}^2 & ... & w_{j,1}^{r-1} \\ 1 & w_{j,2}^1 & w_{j,2}^2 & ... & w_{j,2}^{r-1} \\ ... & ... & ... & ... & ... \\ 1 & w_{j,r}^1 & w_{j,r}^2 & .... & w_{j,r}^{r-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & ... & 1 \\ w_{j,1}^1 & w_{j,2}^1 & ... & w_{j,r}^1 \\ w_{j,1}^2 & w_{j,2}^2 & ... & w_{j,r}^2 \\ ... & ... & ... & ... \\ w_{j,1}^{r-1} & w_{j,2}^{r-1} & ... & w_{j,r}^{r-1} \end{vmatrix} = \prod_{r \ge i > \tau \ge 1} (w_{j,i} - w_{j,\tau}).$$

This a Vandermonde determinant, for $w_{j,i} \ne w_{j,\tau}$, so $|A| \ne 0$, and, therefore, the linear equations have a unique solution $c_0, c_1 .... c_r$.

If $\eta_{i,h} < \eta_{j,h}$ this means that u_i does not have enough attribute permission values $K_{j,1} = t_{j,1}g_1, K_{j,2} = t_{j,2}g_1, ..., K_{j,r} = t_{j,r}g_1$. Assume u_i does not have attribute permission value $K_{j,r} = t_{j,r}g_1$, that is, it cannot compute $w_{j,r}$. According to the point pair $\{(w_{j,1}, y_{j,1}), (w_{j,2}, y_{j,2}), ..., (w_{j,r-1}, y_{j,r-1})\}$, u_i cannot construct polynomial $c_0 + c_1 w_{j,r}^1 + c_2 w_{j,r}^2 + ... + c_{r-1} w_{j,r}^{r-1} = y_{j,r}$, and only construct a linear system of equations with unknown numbers $c_0, c_1 .... c_r$:

$$\begin{cases} c_0 + c_1 w_{j,1}^1 + c_2 w_{j,1}^2 + ... + c_{r-1} w_{j,1}^{r-1} = y_{j,1} \\ c_0 + c_1 w_{j,2}^1 + c_2 w_{j,2}^2 + ... + c_{r-1} w_{j,2}^{r-1} = y_{j,2} \\ ..... \\ c_0 + c_1 w_{j,r-1}^1 + c_2 w_{j,r-1}^2 + ... + c_{r-1} w_{j,r-1}^{r-1} = y_{j,r-1}. \end{cases}$$

There is no solution to this linear system of equations. Thus, u_i cannot get decryption key M_j by solving polynomial functions to decrypt the ciphertext information c_j. □

Theorem 4. *proposed AC-CAATP protocol is security against passive adversary under the DBDH problem assumption. That is, under the DBDH assumption, for any $a, b, c \in \mathbb{Z}_q^*$, $g_1 \in G_1$, $g_2 \in G_2$ and $\pi \in G_2$, there are two computationally indistinguishable tuples $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$ and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$. Even if adversary $\mathcal{C}$ obtains relevant information $\{\eta_{j,h}, T_{j,1}, T_{j,2}, ..., T_{j,r}\}$ from the registration process of AC-CAATP in Table 1 and the information $\{u_j, pk_{u_j}, Keywords_j, D_j, PK_{g-u_j}, c_j, \eta_{i,h}, (y_{j,1}, y_{j,2}, ..., y_{j,r})\}$ through the public display platform in Table 2, it cannot obtain the plaintext information $m = V_j \oplus H_3(e(v_j, M_j))$ without the decryption key M_j.*

Proof. Since $T_{j,\tau} = t_{j,\tau}\lambda_j g_1 (0 \le \tau \le r)$, $T_{pri} = (t_{j,1} + ... + t_{j,r})\lambda_j g_1$, $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + ... + t_{j,r})g_1$, $p_{u_j} = m_j \lambda_j g_1$, $M_j = m_j T_{pri}$, where $m_j \in \mathbb{Z}_p^*$. The ciphertext information is $c_j = (v_j, V_j)$, where

$v_j = \varsigma_j PK_A$, $\varsigma_j \in \mathbb{Z}_p^*$ and $V_j = m \oplus H_3((e(p_{u_j}, \eta_{j,h})^{\varsigma_j})$. $\mathcal{C}$ does the following algorithm $\mathcal{A}$; it selects (ρ_1, ρ_2, ρ_3) from $\mathbb{Z}_p^*$ randomly and computes $f_1 = \rho_1 T_{j,1} = \rho_1 \lambda_j t_{j,1} g_1, f_2 = \rho_1 T_{j,2} = \rho_1 \lambda_j t_{j,2} g_1, f_r = \rho_1 T_{j,r} = \rho_1 \lambda_j t_{j,r} g_1$, $M_j^{'} = f_1 + f_2 + ... + f_r = \rho_1 (t_{j,1} + t_{j,1} + ... + t_{j,1}) \lambda_j g_1 = \rho_1 a g_1$, $v_j^{'} = \rho_2 PK_A$, $\eta_{j,h}^{'} = \rho_3 PK_A$ and $p_{u_j}^{'} = \rho_1 T_{j,0} = \rho_1 c g_1$. If $e(p_{u_j}, \eta_{j,h})^{\varsigma_j} = e(M_j^{'}, V_j^{'})$, this means $\rho_1 = m_j$, $\rho_2 = \varsigma_j$ and $\rho_2 = t_{j,1} + t_{j,1} + ... + t_{j,1}$. Then, we can construct another algorithm $\mathcal{A}'$ to call $\mathcal{A}$ to efficiently distinguish $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$ and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$, where $ag_1 = (T_{j,1} + T_{j,2} + ... + T_{j,r}) = (t_{j,1} + t_{j,2} + ... + t_{j,r}) \lambda_j g_1$, $bg_1 = V_j = \varsigma_j PK_A = \rho_3 PK_A$ and $cg_1 = T_{j,0} = \lambda_j g_1$, which is a contradiction for the DBDH problem assumption. Thus, the proposed protocol is secure against passive attacks under the DBDH problem assumption. □

Theorem 5. *Our proposed scheme can defend against collusion attacks. Anyone who does not have sufficient attribute rights can't collude to access resources beyond their access rights.*

Proof. On the one hand, each member's permission parameters are different, even if they are the same attribute; this means, even if $T_{j,1} = T_{j,1}$, $a_{i,1}$ is not equal to $a_{j,1}$, and u_i cannot obtain the attribute $a_{j,1}$ from $T_{j,1}$ in CS platform. On the other hand, each member obtains a privilege grade $\eta_{i,h}$ according to its own attribute when registering the identity. When accessing the resource, the CS perform joint authentication on the identity and privilege grade of the resource visitor by the equation $e(\eta_{i,h}, pk_{u_i}) = e(\sigma_i, PK_A)$, and prohibits the user to access certain resources for which its privilege grade does not meet the requirements for accessing the resource. □

6. Efficiency Analysis

Computational consumption, storage space, and communication load are three important indicators for measuring the performance of access control protocols. According to the analytical data provided by [27], this section compares the proposed scheme with [27,31] in the three performance indicators.

References [27,31] adopt a tree-structured access control scheme. For discussion conveniences, according to the expression of [31], suppose n_u is the average number of attributes per user, n_c is the average number of attributes associated with the policy tree of ciphertext, $|tr|$ is the average number of translation nodes in a ciphertext, and $|tr_{Attr}|$ is the average number of necessary translation nodes for the network attribute set $Attr$.

6.1. Computation Overhead

In terms of computing load, the two most important calculations include bilinear pairing operation and exponential operation, since, compared with pairing and exponentiation operation, the cost of addition and multiplication operation can be neglected. Assume there are n members participating in system resource sharing. T_{bp} denotes the cost of the bilinear pairing operation on group G_1, T_{exp} denotes the cost of the exponentiation operation, and $n_{c,u}$ represents the average number of attributes that each user uses to decrypt the ciphertext. $n_{c,Attr}$ represents the average number of attributes used to decrypt ciphertext by a set of users with attribute set $Attr$, and $|Attr|$ denotes the number of attributes in set $Attr$. $|nl|$ represents the average number of non-leaf nodes when computing the secret from leaf nodes to root node according to access policies. The computation load comparison for our scheme and other two schemes as shown in Table 3.

Table 3. Symbols used mainly in this chapter.

Phase	Bethencourt et al. [27]	Xue et al. [31]	Li et al. [15]	Zhong et al. [19]	Ours
Setup	$3T_{\exp} + T_{bp}$	$(5+n)T_{\exp} + T_{bp}$	$(2n_u + 4)T_{exp} + 1T_{bp}$	$2n_u T_{exp} + n_u T_{bp}$	$2n_u \lvert Attr \rvert T_{\exp} + 4T_{bp}$
KeyGen	$(2n_u + 2)T_{\exp}$	$(2n_u + 3)T_{\exp}$	$3n_u T_{exp} + n_u T_{bp}$	$3n_u T_{exp}$	$n_u T_{exp}$
Encrypt	$(2n_c + 2)T_{exp}$	$(2n_c + 3 + \lvert tr \rvert)T_{exp}$	$(4n_u + 1)T_{exp} + 1T_{bp}$	$4T_{exp} + 4T_{bp}$	$4T_{bp}$
Decrypt	$(2n_{c,u} + 1)T_{bp} + (n_{c,u} + \lvert nl \rvert)T_{\exp}$	$(2n_{c,Attr} + \lvert tr_{Attr} \rvert + 2)T_{bp} + (n_{c,Attr} + \lvert nl \rvert)T_{\exp}$	$3n_u T_{bp}$	$1T_{exp} + 3T_{bp}$	$3T_{bp}$

From Table 3, for the comparative analysis of the five schemes in terms of the total calculation amount, the total calculation amount of our scheme is the smallest, followed by the scheme Zhong et al. [19]. The calculation amounts of Xue et al. [31] and Li et al.[15] are relatively large. In the initialization phase, because the terminal nodes of the IoT network may be increased, the calculation amount of Xue et al. [31] increases linearly with the increase of network nodes. Our scheme is larger than that of the other three schemes, mainly because our scheme performs attribute encryption authentication in the initialization phase, ensuring that personal attributes are not leaked, protecting personal privacy and higher security. The other four schemes do not have this feature. In the KeyGen phase, our scheme is the smallest, followed by the scheme Bethencourt et al. and Xue et al. [31]. They have the same calculation amount. The scheme of Li et al. [15] is the largest. In the Encrypt and Decrypt phase, our scheme and Zhong et al. [19] are the smallest, followed by the scheme of Bethencourt et al. [27] and Li et al. [15]. The calculation amount of Xue et al. [31] is the largest.

6.2. Computation Time Cost

We analyze how the execution time as the number of node attributes grows in each phase, which runs the related algorithm through program pbc-0.5.12 provided by the Pairing Based Cryptography Library(PBC), on an environment of Intel(R) Core(TM)2 Duo E8400 CPU(3.00 GHz) (LENOVO (Being) LIMITED, Beijing, China), Ubuntu 10.04, the average run time of the multiplication on G_1 is 0.016 ms, and the average exponent operation time of G_1 and G_2 are 3.886 ms and 0.489 ms, respectively, and the average run time of the bilinear pair is 4.354 ms. Because the execution time of multiplication is about 0.005 times that of the other three algorithms, the multiplication operation can be ignored in our analysis. For the convenience of discussion, we assume that the number of nodes in the network is 150, and the number of attributes in the network attribute set $Attr$ is 8, all the attributes constitute a binary policy tree, all the attributes associated with the policy tree of ciphertext to decrypt ciphertexts, and all the non-leaf nodes as necessary translation nodes. The execution times of each phase in the five schemes are shown in Figures 2–5, respectively.

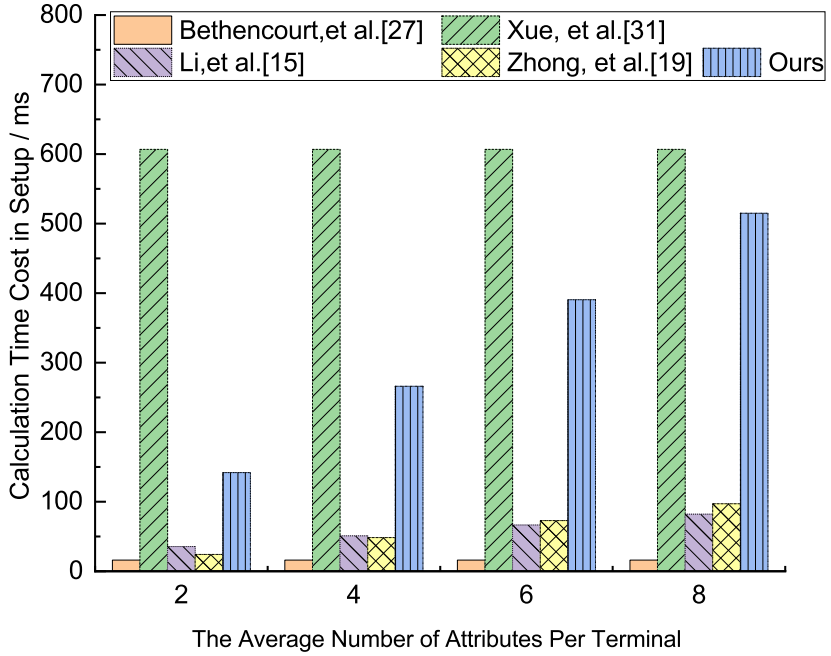

Figure 2. Calculation time cost comparison analysis in the setup phase of the five protocols.

From Figure 2, the comparative analysis of the five schemes in terms of the calculation time in the setup phase. For these five schemes, the scheme of Xue et al. [31] is the longest, followed by Ours. The scheme of Bethencourt et al. [27] has the least calculation time, followed by Li et al. [15] and Zhong et al. [19], their calculation time is similar. In this phase, our scheme performs attribute encryption authentication in the initialization phase, ensuring that personal attributes are not leaked, protecting personal privacy, and higher security. The other four schemes do not have this feature.

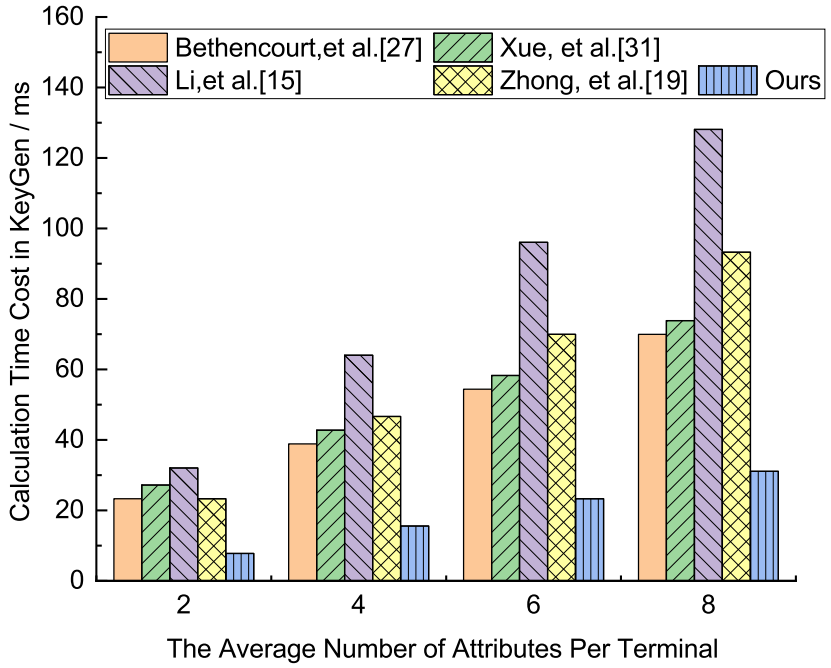

Figure 3. Calculation time cost comparison analysis in the key generation phase of the five protocols.

From Figure 3, the comparative analysis of the five schemes in terms of the calculation time in the key generation phase. For these five schemes, the scheme of Li et al. [15] is the longest, followed by

Zhong et al. [19]. The scheme of ours has the least calculation time, followed by Xue et al. [31] and Bethencourt et al. [27], their calculation time is similar.

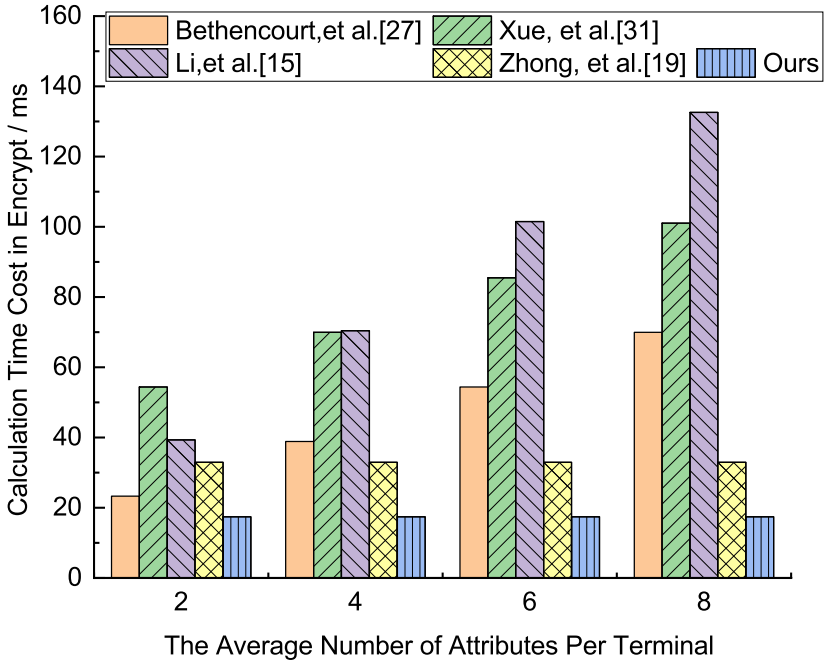

Figure 4. Calculation time cost comparison analysis in the encryption phase of the five protocols.

From Figure 4, the comparative analysis of the five schemes in terms of the calculation time in the encryption phase. For these five schemes, the scheme of Li et al. [15] is the longest, followed by Xue et al. [31]. The scheme of ours has the least calculation time, followed by Zhong et al. [19]. The calculation time of Bethencourt et al. [27] is in the middle of the five schemes.

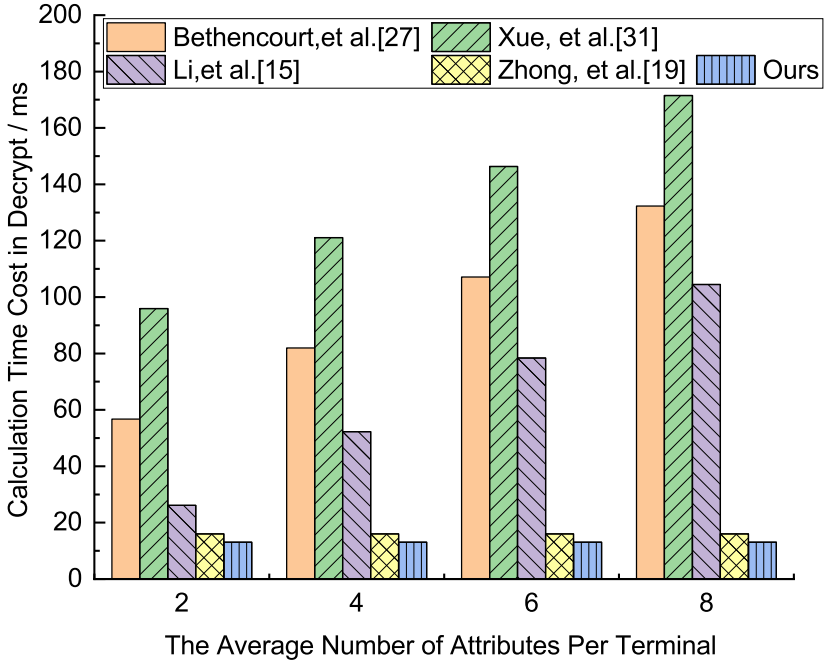

Figure 5. Calculation time cost comparison analysis in the decryption phase of the five protocols.

From Figure 5, the comparative analysis of the five schemes in terms of the calculation time in the decryption phase. For these five schemes, the scheme of Xue et al. [31] is the longest, followed

by Bethencourt et al. [27]. The scheme of ours and Zhong et al. [19] has the least calculation time, their calculation time is similar. The calculation time of Li et al. [15] is in the middle of the five schemes.

7. Conclusions

When sharing data resources in the Internet of Things, it is of great significance to encrypt the data and set threshold functions to control the access rights of users to protect the security of the data. Information resource sharing based on the Internet of Things is highly vulnerable to external or internal threats. The complex access environment of the Internet of Things makes it easy for users' privacy and shared resource information to be leaked or maliciously attacked. Therefore, appropriate measures must be taken to make information resource sharing more secure and reliable. This paper proposes an access control scheme based on ciphertext attribute authentication and threshold function for IoT resource sharing. Firstly, it introduces the application background and existing security challenges of the Internet of Things. Secondly, it analyzes and summarizes the relevant international research results, and introduces the research contribution of this paper. Thirdly, in order to describe the introduction of the proposed algorithm and research scheme in more detail, the main technology is to propose ciphertext identity authentication based on attribute encryption technology, which can achieve the purpose of identity authentication, and also can effectively protect the privacy of terminal members. For the information resources to be shared by the terminal members, the resource information is encrypted before being uploaded to the cloud server to prevent the terminal members who do not have the rights to access the information resources, and at the same time ensure the confidentiality and security of the data during the transmission process. When accessing data resources, set access rights to terminal members, and use attribute-based threshold functions to set access permission levels for each terminal member. Divide different permission levels according to different attributes of users, access information resources of different sensitivity levels, avoid leakage of sensitive information, and make access to information resources more flexible and quickly. Finally, the correctness and security of the proposed scheme are proved, and the computational complexity and computational time overhead of the scheme are analyzed. The proposed scheme is applicable to the resource access control of small mobile devices with limited IoT resources.

Author Contributions: Q.Z., J.Y. and Y.G. conceived and designed the experiments; Y.L. and X.L made graphs and tables; Z.L. and Y.G. collected data; X.L., Z.L. and Q.Z. analyzed the data; Y.L. searched related articles; Q.Z. and Y.L. wrote the paper.

Funding: This work is supported by the National Natural Science Foundation of China under Grant Nos. 61772477 and 61971380, the PhD Research Fund of the Zhengzhou University of Light Industry, and the Research Foundation of Beijing Institute of Technology (20120742012) and U1804263.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Pau, G.; Bazzi, A.; Campista, M.E.M.; Balador, A. Towards 5G and beyond for the internet of UAVs, vehicles, smartphones, Sensors and Smart Objects. *J. Netw. Comput. Appl.* **2019**, *135*, 108–109.
2. Pau, G.; Chaudet, C.; Zhao, D.; Collotta, M. Next, generation wireless technologies for internet of things. *Sensors* **2018**, *18*, 221.
3. Karray, F.; Jmal, M.W.; Garcia-Ortiz, A.; Abid, M.; Obeid, A.M. A comprehensive survey on wireless sensor node hardware platforms. *Comput. Netw.* **2018**, *144*, 89–110.
4. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib.* **2012**, *24*, 131–143.
5. Bertin, E.; Hussein, D.; Sengul, C.; Frey, V. Access control in the Internet of Things: a survey of existing approaches and open research questions. *Ann. Telecommun.* **2019**, *74*, 357
6. Li, W.; Xue, K.; Xue, Y.; Hong, J. TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *27*, 1484–1496.

7. Saia, R.; Carta, S.; Recupero, D. A Probabilistic-driven Ensemble Approach to Perform Event Classification in Intrusion Detection System. In Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Seville, Spain, 18–20 September 2018; pp. 139–146.
8. Saia, R.; Carta, S.; Recupero, D.R.; Fenu, G.; Stanciu, M.M. A Discretized Extended Feature Space (DEFS) Model to Improve the Anomaly Detection Performance in Network Intrusion Detection Systems. In Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Vienna, Austria, 17–19 September 2019; pp. 322–329.
9. Arrington, B.; Barnett, L.; Rufus, R.; Esterline, A. Behavioral modeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms. In Proceedings of the 25th International Conference on Computer Communication and Networks (ICCCN), Waikoloa, HI, USA, 1–4 August 2016; pp. 1–6.
10. Pau, G.; Arena, F. An overview of vehicular communications. *Future Internet* **2019**, *11*, 27.
11. Saia, R.; Carta, S.; Recupero, D. R.; Fenu, G. Internet of entities (IoE): A blockchain-based distributed paradigm for data exchange between wireless-based devices. In Proceedings of the 8th International Conference on Sensor Networks, Prague, Czech Republic, 26–27 February 2019; pp. 77–84.
12. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A Novel Attribute-Based Access Control Scheme Using Block chain for IoT. *IEEE Access* **2019**, *7*, 38431–38441.
13. El Sibai, R.; Gemayel, N.; Bou Abdo, J.; Demerjian, J. A survey on access control mechanisms for cloud computing. *Trans. Emerg. Telecommun. Technol.* **2019**, doi:10.1002/ett.3720.
14. Pal, S.; Hitchens, M.; Varadharajan, V.; Rabehaja, T. Policy-based access control for constrained healthcare resources in the context of the Internet of Things. *J. Netw. Comput. Appl.* **2019**, *139*, 57–74.
15. Li, B.; Huang, D.; Wang, Z.; Zhu, Y. Attribute-based access control for ICN naming scheme. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 194–206.
16. Li, Q.; Zhu, H.; Xiong, J.; Mo, R.; Ying, Z.; Wang, H. Fine-grained multi-authority access control in IoT-enabled mHealth. *Ann. Telecommun.* **2019**, *74*, 389–400.
17. Pugazhenthi, A.; Chitra, D. Data Access Control and Secured Data Sharing Approach for Health Care Data in Cloud Environment. *J. Med. Syst.* **2019**, *43*, 258.
18. Shanmugapriya, E.; Kavitha, R. Efficient and Secure Privacy Analysis for Medical Big Data Using TDES and MKSVM with Access Control in Cloud. *J. Med. Syst.* **2019**, *43*, 265.
19. Zhong, H.; Zhu, W.; Xu, Y.; Cui, J. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Comput.* **2018**, *22*, 243–251.
20. Xu, S.; Yang, G.; Mu, Y.; Liu, X. A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Gener. Comput. Syst.* **2019**, *97*, 284–294.
21. Habib, M.A.; Ahmad, M.; Jabbar, S.; Khalid, S.; Chaudhry, J.; Saleem, K.; Rodrigues, J.J.; Khalil, M.S. Security and privacy based access control model for internet of connected vehicles. *Futur. Comput. Syst.* **2019**, *97*, 687–696.
22. Haddada, L.; Essoukri, N. Double watermarking-based biometric access control for radio frequency identification card. *Int. Microw. Comput. Aided Eng.* **2019**, doi:10.1002/mmce.21905.
23. Shi, M.; Jiang, R.; Hu, X.; Shang, J. A privacy protection method for health care big data management based on risk access control. *Health Care Manag. Sci.* **2019**, *23*, 1–16.
24. Daoud, W.B.; Obaidat, M.S.; Meddeb-Makhlouf, A.; Zarai, F.; Hsiao, K.F. TACRM: trust access control and resource management mechanism in fog computing. *Hum. Centric Comput. Inf. Sci.* **2019**, *9*, 28.
25. Wang, Q.; Wang, H.; Wang, Y.; Guo, R. A Distributed Access Control with Outsourced Computation in Fog Computing. *Secur. Commun. Netw.* **2019**, doi:10.1155/2019/6782753.
26. Amini, M.; Osanloo, F. Purpose-based privacy preserving access control for secure service provision and composition. *IEEE Trans. Serv. Comput.* **2019**, *12*, 604–620.
27. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 20–23 May 2007; pp. 321–334.
28. Ullah, F.; Anwar, H.; Shahzadi, I.; Ur Rehman, A.; Mehmood, S.; Niaz, S.; Mahmood Awan, K.,; Khan, A.; Kwak, D. Barrier Access Control Using Sensors Platform and Vehicle License Plate Characters Recognition. *Sensors* **2019**, *19*, 3015.

29. Maesa, D.; Mori, P.; Ricci, L. A blockchain based approach for the definition of auditable Access Control systems. *Comput. Secur.* **2019**, *84*, 93–119.
30. Premkamal, P.; Pasupuleti, S.; Alphonse, P. A new verifiable outsourced ciphertext-policy attribute based encryption for big data privacy and access control in cloud. *J. Ambient. Humaniz. Comput.* **2019**, *10*, 2693–2707.
31. Xue, Y.; Xue, K.; Gai, N.; Hong, J.; Wei, D.S.; Hong, P. An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2917–2942.
32. Kanimozhi, S.; Kannan, A.; Suganya Devi, K.; Selvamani, K. Secure cloud-based e-learning system with access control and group key mechanism. *Concurr. Comput. Pract. Exp.* **2019**, e4841, doi:10.1002/cpe.4841.
33. Mahmood, G.; Huang, D.; Jaleel, B. A Secure Cloud Computing System by Using Encryption and Access Control Model. *J. Inf. Process. Syst.* **2019**, *15*, 538–549.
34. Zhu, Y.; Huang, R.; Tao, Y.; Wang, X. An edge re-encryption-based access control mechanism in NDN. *Trans. Emerg. Telecommun. Technol.* **2019**, e3564, doi:10.1002/ett.3565.
35. Sun, G.; Wang, K.; Yu, H.; Du, X.; Guizani, M. Priority-based medium access control for wireless body area networks with high-performance design. *IEEE Internet Things J.* **2019**, *6*, 5363–5375.
36. Grippa, P.; Schilcher, U.; Bettstetter, C. On access control in cabin-based transport systems. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 2149–2156.
37. Lu, B.; Wang, L.; Liu, J.; Zhou, W.; Guo, L.; Jeong, M.H.; Wang, S.; Han, G. LaSa: Location Aware Wireless Security Access Control for IoT Systems. *Mob. Networks Appl.* **2019**, *24*, 748–760.
38. Sindiren, E.; Ciylan, B. Application model for privileged account access control system in enterprise networks. *Comput. Secur.* **2019**, *83*, 52–67.
39. Yan, H.; Wang, Y.; Jia, C.; Li, J.; Xiang, Y.; Pedrycz, W. IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT. *Futur. Comput. Syst.* **2019**, *95*, 344–353.
40. Ali, B.; Awad, A. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817.
41. Tomić, I.; McCann, J. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet Things J.* **2017**, *4*, 1910–1923.