AESM^2 Attribute-Based Encrypted Search for Multi-Owner and Multi-User Distributed Systems

Wang, Mingyue; Miao, Yinbin; Guo, Yu; Huang, Hejiao; Wang, Cong; Jia, Xiaohua

Published in:
IEEE Transactions on Parallel and Distributed Systems

Published: 01/01/2023

Document Version:
Post-print, also known as Accepted Author Manuscript, Peer-reviewed or Author Final version

Publication record in CityU Scholars:
Go to record

Published version (DOI):
10.1109/TPDS.2022.3216320

Publication details:

Citing this paper
Please note that where the full-text provided on CityU Scholars is the Post-print version (also known as Accepted Author Manuscript, Peer-reviewed or Author Final version), it may differ from the Final Published version. When citing, ensure that you check and use the publisher's definitive version for pagination and other details.

General rights
Copyright for the publications made accessible via the CityU Scholars portal is retained by the author(s) and/or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights. Users may not further distribute the material or use it for any profit-making activity or commercial gain.

Publisher permission
Permission for previously published items are in accordance with publisher's copyright policies sourced from the SHERPA RoMEO database. Links to full text versions (either Published or Post-print) are only available if corresponding publishers allow open access.

Take down policy
Contact lbscholars@cityu.edu.hk if you believe that this document breaches copyright and provide us with details. We will remove access to the work immediately and investigate your claim.

https://doi.org/10.1109/TPDS.2022.3216320.
AESM²: Attribute-based Encrypted Search for Multi-owner and Multi-user Distributed Systems

Mingyue Wang, Yinbin Miao, Yu Guo, Heijiao Huang, Cong Wang, Fellow, IEEE, and Xiaohua Jia, Fellow, IEEE

Abstract—With the rapid development of cloud computing, it is popular for data owners to outsource massive data to the cloud server for data sharing. To protect the privacy of sensitive data, many searchable encryption schemes are proposed. However, most of the existing studies focus on the single-owner model. In practice, users need to query data from distributed owners one by one, which inevitably brings great communication and computation overheads. Moreover, it lacks a secure scheme that realizes the access control requirements of individual owners. In this paper, we propose AESM², a new attribute-based encrypted search with ownership enhancement scheme for multi-owner and multi-user distributed systems. Our design enables users to search data from authorized owners with only one trapdoor. Owners can enforce owner level permission on users and encrypt their data individually with fine-grained attribute level permission. For practical consideration, we further devise an efficient revocation method of the owner level permission for users, where ciphertexts do not need to be updated. We formally define and prove the security of our design. Moreover, we implement a system prototype and analyze the performance from theoretical and experimental aspects. The evaluation results demonstrate that our scheme is effective and efficient.

Index Terms—Searchable encryption, attribute-based encryption, access control, multi-owner distributed systems

1 INTRODUCTION

Cloud computing has been widely used by organizations and individuals to have data storage and access services in the big data era. By outsourcing a large volume of data to the cloud server, such as Google Cloud, Aliyun, and Amazon Cloud, the storage burden of the user side can be greatly reduced. However, there are great risks of privacy leakage or unauthorized data access in data outsourcing. With the increasing concerns about data privacy, the encryption-before-outsourcing mechanism is widely adopted in cloud computing.

Data utilization is an important issue with encrypted data. Searchable Encryption (SE) technique [1] provides a promising solution, which allows users to search over the encrypted data without decryption directly. To enrich the functionality and security of SE, many studies have been proposed, such as conjunctive keyword search [2], order-revealing encryption [3], and range queries [4]. However, these schemes only support the single-owner and single-user model, where the user that queries data is also the data owner that outsources data to the server. A more common data-sharing model is that multiple users access data owned by multiple distributed owners (multi-owner/multi-user model). An application example is that many geographically distributed hospitals choose to outsource their data to the same cloud service provider (server). For better diagnosis and treatment, a user (e.g., a doctor) in one hospital needs to access the medical data from other hospitals for the same patient. The common practice is to search data from multiple distributed hospitals.

The multi-owner model can be easily achieved by letting users submit a query to each owner one by one. But it brings high costs in communication and computation for the users. The ultimate goal of the multi-owner and multi-user model is to match a user query with the ciphertexts encrypted by multiple distributed owners. Intuitively, there are two ways to do it. One approach is to let all owners share the same secret key for data encryption. This is not desirable for owners as they would worry about data abuse due to the share of the secret key. The other method is to allow owners to use their own secret keys but requires a trusted third party to convert all ciphertexts with an intermediate key [5]–[7]. This method is inefficient because it is time-consuming to convert ciphertexts, which incurs a high cost of re-encryption. There is also some literature that supports secure multi-owner data sharing [8]–[11]. In [9], it focus on set computation of multiple owners. The scheme in [10] deals with fairness during the search process. However, none of them can meet the access control requirements for individual owners’ datasets. Thus, it is a challenging issue to develop a secure and practical data sharing system for the multi-owner and multi-user model.

Unlike the single-owner model, the privacy issue in the multi-owner model is much more complex, including data privacy and data ownership. The data sharing scheme...
should protect data privacy and also follow access control requirements of owners. For instance, in the medical example mentioned before, different hospitals (owners) have their own access authorization mechanisms, including owner level permission and attribute level permission. Doctors (users) with attributes can access data records from multiple hospitals. For a user, owner level permission means whether it is allowed to search the data of certain owners. The attribute level permission is made by each owner to specify the availability of data record level based on attribute. In such a model, asymmetric cryptography is more suitable for generating ciphertexts with different public keys. For instance, [12] proposed an attribute-based keyword search scheme for the multi-owner and multi-user model. However, it requires the server to hold the user list for each owner. Moreover, owner level permission revocation is another difficult issue in the multi-owner model. The challenge lies in how to update the access capability of users in an efficient manner when their keys are revoked.

In this paper, we propose AESM\textsuperscript{2}, a privacy-preserving Attribute-based Encrypted Search scheme for Multi-owner and Multi-user distributed systems. In our design, we enhance owners’ ownership by utilizing a two-level access control mechanism, i.e., the owner level permission and attribute level permission. To enable users to search over multiple ciphertexts encrypted by different owners, we design a key aggregate search protocol by using the aggregate key technique in [13], [14]. With the authorized aggregate key, the encrypted keyword (trapdoor) from a user can be converted to match multiple ciphertexts, where the access permission of each owner will be checked. For the attribute level permission, keywords of data records are encrypted by the access policy tree structure [15] of different owners. Furthermore, we devise a version-based scheme for efficient key updating when the revocation happens in owner level permission set of the user. It can prevent revoked users from accessing data with old keys without involving any re-encryption. We summarize our contributions as follows.

- We propose a secure attribute-based encrypted search scheme with ownership enhancement for multi-owner and multi-user distributed systems, where users can search the data of authorized owners with one trapdoor.
- We design an efficient revocation method of the owner level permission that prevents revoked users from accessing data with the old keys.
- We define the security model and give a formal security analysis. We implement a system prototype and analyze the experimental evaluation using the real-world dataset, which shows the efficiency of our design.

The rest of this paper is organized as follows. Section 2 surveys related work. Section 3 presents preliminaries. Section 4 describes the problem formulation. We present the detailed construction of AESM\textsuperscript{2} in Section 5. The security analysis is shown in Section 6. We evaluate the performance by theoretical and experimental analysis in Section 7. Finally, Section 8 concludes this paper.

2 RELATED WORK
This paper involves several techniques from applied cryptography. In this section, we review Searchable Encryption and Attribute-based Encryption technologies.

2.1 Searchable Encryption
Research on Searchable Encryption (SE) has experienced a big boom with the rapid development of cloud computing [16]. SE enables the untrusted server to search directly on the outsourced encrypted data without decryption. Song et al. [1] first proposed the concept of symmetric searchable encryption (SSE), which motivated a great quantity of further research works in this field [2], [17], [18]. In the following, Boneh et al. [17] presented the first public-key encryption with keyword search. In [18], Li et al. enriched the functionality of fuzzy encrypted keyword search. Cash et al. [2] devised the first SSE scheme for boolean keyword search with sublinear complexity. However, these designs only apply to the single-user setting where the data owner (i.e., user) outsources and searches data with its own secret key. To bridge the gap, multi-user SE [19]–[21] has also been extensively studied, where multiple users can perform search operations. For example, Sun et al. [20] devised a non-interactive authorization SE scheme for multiple clients.

However, these works do not provide fine-grained access control on data records for users. To achieve such a goal, Popa et al. [22] proposed the notion of multi-key searchable encryption, which allowed authorized users to search over multiple files encrypted by different keys with a single request. Unfortunately, Tang et al. [23] showed the security vulnerability when the server collided with a malicious user and proposed an improved scheme. Following this direction, Cui et al. [13] designed the Key-Aggregate Searchable Encryption (KASE) scheme, which can support data sharing within a group. Later, Zhou et al. [14] pointed out that there existed keyword guessing attacks by unauthorized inside users in [13] and solved this problem. But these schemes only allow a single owner to outsource encrypted data, which does not apply to the multi-source data scenarios (e.g., task recommendation services of crowdsourcing [24]). In the multi-owner and multi-user data-sharing model, users need to access data from multiple data owners. To achieve this goal, Bao et al. [5] adopted a trusted administration server as the middleware to transform indexes and trapdoors, which brings expensive computation. According to application scenarios, in [8], owners can share their data with users in the same group. Huang et al. [25] proposed a conditional dissemination scheme for co-owner data group sharing. Very recently, Wang et al. [11] designed a hybrid searchable encryption technique where multiple writers (owners) serve one specific reader (user). Nevertheless, these studies mentioned above do not consider individual access control requirements of each owner’s dataset, which is the focus of this paper (AESM\textsuperscript{2}). We do not consider the access pattern issue, which can be extended with ORAM [26] or volume hiding [27] techniques.

2.2 Attribute-based Encryption
Due to the property of fine-grained access control for multiple users, there have been extensive research findings on attribute-based encryption (ABE) [29]–[32]. ABE allows
users with appropriate secret keys to decrypt ciphertexts encrypted under access policies. According to how the ciphertext is encrypted, there are two complementary forms of ABE: Key-Policy ABE (KP-ABE) [33] and Ciphertext-Policy ABE (CP-ABE) [29], [34]. In KP-ABE, attributes are used to describe ciphertexts, and access policies over these attributes are associated with secret decryption keys. Instead, in CP-ABE, attributes are utilized to describe secret keys for users, and access policies over these policies are built into ciphertexts.

Goyal et al. [33] first proposed KP-ABE scheme based on the access tree. In the follow-up design, Bethencourt et al. [34] constructed the first CP-ABE, which motivated many works [35]–[38] in data access control applications. Later, a decentralized multi-authority CP-ABE scheme [29] was proposed to solve the access control issue under multiple authorities. To enrich the functionality and improve the security, revocable CP-ABE was presented in [39], where the threshold value of node $v$ is the OR gate. The AND gate can be computed according to $v_{\text{num}}$, let $q_{\text{root}}(0)$ denote the parent node of $v$.

Given the access tree $T$, we can hide the secret value $s$ according to $T$ by

$$q_{f}(0)_{f \in E(T)} \leftarrow \text{Share}(T,s),$$

where $E(T)$ denotes the set of leaf nodes. For each node $v$, it generates a polynomial $q_v$ of degree $k_v - 1$ (leaf node $k_v = 1$) in a top-down manner. If node $v$ is the root of $T$, $q_v(0) = s$. Otherwise, it sets $q_v(0) = q_{p(v)}(\text{ind}(v))$, where $p(v)$ denotes the parent node of $v$.

Given a value set $\{E_{u_1}, \ldots, E_{u_m}\}$ with the leaf node set $\{u_1, \ldots, u_m\}$ of access tree $T$. For $j \in \{1, \ldots, m\}$, $q_{u_j}(0)$, ..., $q_{u_j}(\text{num}_v)$ are the secret shares of the secret value $s$ distributing according to $T$. $F(\text{Atts}, T) = 1$, $E_{u_j} = e(g,g)^{q_{u_j}(0)}$, the element secured in root node $E_{\text{root}} = e(g,g)^{q_{\text{root}}(0)} = e(g,g)^s$ can be reconstructed in a bottom-up manner as

$$e(g,g)^s = \text{Combine}(T, \{E_{u_1}, \ldots, E_{u_m}\}),$$

where $e$ is the bilinear pairing with generator $g$.

### Table 1: Encrypted Multi-owner and Multi-user (M2M) Data Sharing Schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>M2M</th>
<th>Fine-grained Access Control</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mona [8]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>QYWY [25]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>ABKS-SM [28]</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Omnes [11]</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>AESM²</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 3 Preliminaries

In this section, we introduce some security assumptions and background techniques before presenting details of the proposed scheme.

### 3.1 Cryptographic Assumptions

**Bilinear Pairings.** $G$ and $G_T$ are both multiplicative cyclic groups of prime order $p$. Let $g$ and $g_T$ denote the generators of $G$ and $G_T$, respectively. A bilinear pairing $e: G \times G \rightarrow G_T$ has three properties: (1) **Bilinearity.** For all $u,v \in G$, and $a, b \in \mathbb{Z}_p^*$, it satisfies $e(u^a,v^b) = e(u,v)^{ab}$. (2) **Non-degeneracy.** $e(g,g) \neq 1$. (3) **Computability.** It is efficient to compute $e(u,v)$ for any $u,v \in G$.

**Computational Diffie-Hellman (CDH) Assumption.** Let $G$ be a group of prime order $p$. Given the triple $(g,g^{z_1},g^{z_2}) \in G$, the goal of adversary $A$ is to compute $g^{z_1z_2}$. We can say that the CDH assumption holds if there exists no adversary that can solve the CDH problem with non-negligible advantage.

**Generic Bilinear Group Model.** In additive group $\mathbb{Z}_p^+$, we consider two random injective maps $\psi_0, \psi_1: \mathbb{Z}_p^+ \rightarrow \{0,1\}^n$, where $n > 3 \log(p)$. In the groups $G, G_T$ of order $p$, we are given the oracle to compute bilinear map $e: G \times G \rightarrow G_T$, where $G = \{\psi_0(x) | x \in \mathbb{Z}_p^+\}$, $G_T = \{\psi_1(x) | x \in \mathbb{Z}_p^+\}$. We define $G$ as a generic bilinear group.

### 3.2 Access Policy Tree

Access policy can be represented by the access trees [33], consisting of leaf nodes and inner (non-leaf) nodes. A leaf node is associated with an attribute and an inner node is a threshold gate. In access tree $T$, let $T_v$ denote the subtree of $T$ with root at node $v$ (e.g., $T_{\text{root}} = T$). $\text{att}(f)$ represents the attribute of leaf node $f$. The number of children in node $v$ is $\text{num}_v$, and index the children as $E_T(v) = \{1, \ldots, \text{num}_v\}$.

The threshold value of node $v$ is $k_v$, where $1 \leq k_v \leq \text{num}_v$. When $k_v = 1$, it is the OR gate. The AND gate can be represented by $k_v = \text{num}_v$. Let $F(\text{Atts}, T) = 1$ represent that the attribute set $\text{Atts}$ of $\text{att}(f)$ satisfies the access policies of subtree $T_v$.

Given the access tree $T$, we can hide the secret value $s$ according to $T$ by

$$\{q_{f}(0)_{f \in E(T)} \leftarrow \text{Share}(T,s),$$

where $E(T)$ denotes the set of leaf nodes. For each node $v$, it generates a polynomial $q_v$ of degree $k_v - 1$ (leaf node $k_v = 1$) in a top-down manner. If node $v$ is the root of $T$, $q_v(0) = s$. Otherwise, it sets $q_v(0) = q_{p(v)}(\text{ind}(v))$, where $p(v)$ denotes the parent node of $v$.

Given a value set $\{E_{u_1}, \ldots, E_{u_m}\}$ with the leaf node set $\{u_1, \ldots, u_m\}$ of access tree $T$. For $j \in \{1, \ldots, m\}$, $q_{u_j}(0), \ldots, q_{u_j}(\text{num}_v)$ are the secret shares of the secret value $s$ distributing according to $T$. $F(\text{Atts}, T) = 1$, $E_{u_j} = e(g,g)^{q_{u_j}(0)}$, the element secured in root node $E_{\text{root}} = e(g,g)^{q_{\text{root}}(0)} = e(g,g)^s$ can be reconstructed in a bottom-up manner as

$$e(g,g)^s = \text{Combine}(T, \{E_{u_1}, \ldots, E_{u_m}\}),$$

where $e$ is the bilinear pairing with generator $g$.

### 4 Problem Formulation

In this section, we formally describe the target problem of this paper. We present the system model and threat model. The notations used are listed in TABLE 2.
TABLE 2: Notations

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{O} = {o_1, o_2, ..., o_n} )</td>
<td>data owner collection</td>
</tr>
<tr>
<td>( \mathcal{R}_i )</td>
<td>plaintext record collection of owner ( o_i )</td>
</tr>
<tr>
<td>( \mathcal{W}_i = {w_1, w_2, ..., w_m} )</td>
<td>keyword collection of owner ( o_i )</td>
</tr>
<tr>
<td>( pk_{cs}, sk_{cs} )</td>
<td>public key and secret key of cloud server</td>
</tr>
<tr>
<td>( pk_{oi}, sk_{oi} )</td>
<td>public key and secret key of owner ( o_i )</td>
</tr>
<tr>
<td>( u )</td>
<td>authorized user</td>
</tr>
<tr>
<td>( sk_{u,ap} )</td>
<td>owner level permission key for ( u )</td>
</tr>
<tr>
<td>( S )</td>
<td>owner level permission set for user ( u )</td>
</tr>
<tr>
<td>( Attrs )</td>
<td>attribute set of user ( u )</td>
</tr>
<tr>
<td>( sk_{u,att} )</td>
<td>attribute level permission key for user ( u )</td>
</tr>
<tr>
<td>( T_i )</td>
<td>access policy tree of owner ( o_i )</td>
</tr>
<tr>
<td>( C_{i,ap} )</td>
<td>ciphertext of owner permissions of ( o_i )</td>
</tr>
<tr>
<td>( \mathcal{W}_{i,w} )</td>
<td>encrypted keyword ( w ) of owner ( o_i )</td>
</tr>
<tr>
<td>( \hat{w} )</td>
<td>query keyword</td>
</tr>
<tr>
<td>( Tp_{u,w} )</td>
<td>search trapdoor from user ( u )</td>
</tr>
<tr>
<td>( \hat{u} )</td>
<td>user with revoked owner level permission</td>
</tr>
<tr>
<td>( S^* )</td>
<td>permission set after revocation</td>
</tr>
<tr>
<td>( UK_t )</td>
<td>update key of system version</td>
</tr>
<tr>
<td>( sk_{u,ap}^* )</td>
<td>updated owner level permission key for ( \hat{u} )</td>
</tr>
</tbody>
</table>

4.1 System Model

In the multi-owner and multi-user model, there are four entities involved, as depicted in Fig. 1. They are Trusted Authority (authority), Data Owners (owners), Cloud Server (server), and Data Requesters (users).

The authority is responsible for issuing keys to owners, the server, and users. It generates the aggregate owner level permission key for users corresponding to the access permissions from multiple owners. Meanwhile, it grants users attributes according to their identities or roles in the system and assigns the attribute keys.

Each owner has a collection of data records \( \mathcal{R}_i \) and the extracted keyword set \( \mathcal{W}_i \). It defines the access control requirements, including the owner level permission and fine-grained attribute level permission on \( \mathcal{R}_i \) for multiple users. To enable efficient queries on the encrypted records, the owner builds searchable indexes on the keyword set \( \mathcal{W}_i \). In this process, the owner’s predefined access policies are embedded in these indexes to enforce the record-level access control. Then, the owner uploads the encrypted data records and searchable indexes to the server.

The server provides storage and search services. It stores the encrypted records and indexes from owners. After receiving search requests from users, it performs the search protocol and returns the matched encrypted records as results to users.

Each user is associated with a set of attributes and assigned owner level access permission according to its identity and role in the system. When a user searches a keyword \( \hat{w} \), it calculates the corresponding trapdoor (encrypted \( \hat{w} \)) and submits it to the server. It can get all matched results of multiple owners with only single query. Then, it will decrypt these records. The record decryption process is out of the scope of this paper. Readers can refer excellent works in [30], [42].

The access control design is suitable for many practical data-sharing systems, such as electronic medical and university resource-sharing systems. For a medical system, authorizations among multiple hospitals are owner level permissions, which are institution-based. Attribute level permissions are requirements on data records for each user of hospitals that have been authorized. The user’s access to each record depends on its professional title in the authorized hospital.

The problem of our concern is that, given a search trapdoor submitted by a user, the server can search datasets from multiple owners that the user is permitted to access and return the complete results, subject to satisfying the following requirements:

1) **Privacy-preserving encrypted search over data of multiple owners by multiple users.** The proposed scheme should allow the server to search over the encrypted data records without leaking any information about data and the query, where the owner level permission and attribute level permission are enforced.

2) **Owner level permission revocation.** The access permission of each owner should be dynamic. Once user’s access permissions of some owners are revoked, it cannot perform correct search with the previous keys as before.

4.2 Threat Model

In our threat model, we make following threat assumptions regarding to each entity involved:

- **Authority** is considered as fully trusted, and all information is securely exchanged with the authority.
- **Server** is assumed as honest-but-curious as in the previous work [43]. It could perform the designated search operations honestly while it is eager to obtain sensitive information from the ciphertexts of data records and trapdoors. It also attempts to launch keyword guessing attacks using available information. We also assume that the server would not collude with other parties (especially malicious users).
- **Owners** are considered to be fully trusted in the sense that they will protect their keys privately and submit the valid ciphertexts to the server.
- **Users** are assumed as malicious. They could generate valid trapdoors to search for their interested keywords while intend to guess what other users can search (unauthorized insiders guess the private keys of other users) and obtain unauthorized data access.

1. We refer to those users who intend to access data from datasets that owner level permissions have been revoked.
5 Proposed AESM² Scheme

In this section, we first present the overview of our design. Then, we propose the detailed construction of AESM² scheme. After that, we describe revocation method to deal with dynamic changes of owner level permission in multi-owner and multi-user distributed systems.

5.1 Design Overview

In the outsourced multi-owner and multi-user data sharing setting, apart from data privacy, data access authorization is also a fundamental problem. There are two challenging issues yet to be solved. One is how to enable a user to search all encrypted indexes from multiple owners with only one trapdoor. Each owner has individual access control requirements, including the owner level permission and attribute level permission. That is, only when a user has the owner’s access permission can it search data according to the fine-grained attribute level permission. This is difficult because the indexes are encrypted by multiple owners under different access control mechanisms. Intuitively, it can be achieved by submitting search trapdoors to the server one by one. Each trapdoor can be used to search the data of a certain owner. However, this direct method is burdensome for users to generate trapdoor repeatedly (see performance analysis in section 7). Existing solutions [5], [6], [28] did not consider the access requirements of individual owners. The other issue is to enable effective and reliable revocation for users. The challenge lies in how to prevent the user from accessing the data where its owner level permission from some owners is revoked. As owner level permission for the user are flexible, it is hard for the server to judge whether the trapdoor contains the revoked owner level permissions (i.e., trapdoor is generated with the key used before revocation).

To solve the first issue, we start with file-based sharing schemes [13], [22], where the trapdoor can be converted to search multiple files. However, these schemes cannot satisfy access control requirements as desired in our multi-owner setting. To this end, we design a matching protocol based on two-level access permissions. In the owner level permission, we adopt the aggregate key [13], [44] technique to enable the single trapdoor to adapt to multiple indexes. Different from the single-owner setting [13], [14], in our design, these index ciphertexts are encrypted by different keys of multiple owners. Besides, each owner generates its own random nonce to build encrypted indexes. A trusted authority is introduced to aggregate all authorized owner’s access permissions into a single key for the user. During searching, the server uses the aggregate key to identify which datasets of these owners can be accessed by this user. In the attribute level permission, the keyword-record sets are encrypted under the fine-grained access policies by each owner. The queried keyword will be matched if the attributes of the user satisfy the access policy, where the secret value secured by the policy tree can be recovered. The server needs to perform the match operations with the trapdoor and the authorized datasets in the owner level permission to return all matched results for the user.

To deal with the second issue, we assign a version number for each period of revocation in the owner level permission. When the revocation happens, only secret keys need to be updated for users. There are no re-encryption operations on ciphertexts, which incurs no cost for owners in the revocation phase. When the owner level permission of a user (revoked user) is revoked by corresponding owners (revoking owners), the authority generates a new version number and updates all of the users’ secret keys. With the updated key, the revoked users cannot search data from the revoking owners anymore. Non-revoked users can continue having the service with updated secret keys. To improve the system efficiency, we delegate the server to update the system version number for related parameters, such that non-revoked users can also search all the data with unchanged access privileges. Moreover, all users only need to keep the latest secret key instead of all previous keys.

5.2 Construction of AESM²

The construction of proposed AESM² scheme consists of five phases: System Initialization, Key Generation, Index Encryption, Trapdoor Generation and Multi-owner Multi-user Encrypted Search.

5.2.1 System Initialization

The authority sets up the system by running the Setup algorithm with the security parameter as input. It first selects two multiplicative groups $G$, $G_T$ of the same order $p$ and the bilinear pairing $e : G \times G \rightarrow G_T$. To model the security in the random oracles, the authority also needs to choose two hash functions $H_1 : \{0,1\}^* \rightarrow G$, $H_2 : \{0,1\}^* \rightarrow Z_p^*$. $H_1$ maps the strings to elements of group $G$, and $H_2$ is a one-way hash function. Then, it chooses several random elements $a,b,c, \beta_2 \in Z_p^*$ as the system master key $msk = (a,b,c, \beta_2)$. The authority also chooses random elements $\alpha \in Z_p^*$ as the common secret parameters for all owners. It accordingly computes $v = g^{2\beta_2}$, $g_t = g^{(\alpha^t)} (t \in \{1,\ldots,2n\})$, where $n$ is the maximum number of owners in the system. The system public parameter $pp$ is generated as

$$pp = (g, v, g^a, g^b, g^c, \{g_t\}, H_1, H_2).$$

5.2.2 Key Generation

The key generation algorithm KeyGen contains the server’s key generation, owner’s key generation, and user’s key generation.

Server’s Key Generation: To avoid users’ keyword guessing attack [45] by inside attackers [14], it is necessary to assign the server with keys in our scheme AESM². By running KeyGen_{sys} algorithm, the authority first generates a random element $\beta_1 \in Z_p^*$ as the secret key $sk_{sys} = \beta_1$ for the server. It then computes the corresponding public key as

$$p_{sys} = u = g^{\beta_1}.$$

Owner’s Key Generation: For each owner $o_i$, the authority chooses two random elements $\gamma_{i,1}, \gamma_{i,2} \in Z_p^*$ and generates the secret key through the KeyGen_{owner} algorithm as

$$sk_{o_i} = (\gamma_{i,1}, \gamma_{i,2}, e_{k_{i,1}}, e_{k_{i,2}}),$$

where $e_{k_{i,1}} = u^{\gamma_{i,1}} = g^{\beta_1 \gamma_{i,1}}$, $e_{k_{i,2}} = v^{\gamma_{i,1}} = g^{\beta_2 \gamma_{i,1}}$ are the private encryption keys of $o_i$. The authority then computes
that the version number is designed to support owner level
Atts$\to$S
user
owner level permissions from each owner for an authorized
and generates the public keys for owner $o_i$ as
$$pk_{o_i} = \{h_{t,1} \}_{t \in \{1, \ldots, n\}}, \{h_{t,2} \}_{t \in \{1, \ldots, 2n\}}.$$ User’s Key Generation: According to the access control
controls of multiple owners (as introduced in subsection
5.1), the user’s authorization key consists of two parts, owner
level permission key and attribute level permission key. It is generated by running the $KeyGen_{user}$ algorithm
for a user.

After choosing a permission version number as $VN = ver$, the authority first generates the aggregate key $sk_{u,ap}$ of
owner level permissions from each owner for an authorized
user $u$ as
$$sk_{u,ap} = \prod_{k \in S} g_{n+1-k}^{\beta_{k,ver}},$$ where $S \in \{1, \ldots, n\}$ represents the owner set authorized

to $u$. If a user gets no access permissions from owners (i.e., $S = \emptyset$), it will not obtain this secret key. It is worth noticing
that the version number is designed to support owner level
permission revocation (to be discussed in subsection 5.3).
According to the identity or role of user $u$, the authority
entitles a set of attributes $Atts$ to $u$. Then, the authority
generates random elements $r \in Z_p^*$ and $r_j \in Z_p^*$ for
each attribute $at_j \in Atts$. It computes the attribute level
permission key $sk_{u,att}$ for user $u$ as
$$sk_{u,att} = \{sk_{u,ap}, sk_{u,att} \} \text{ together with } S \text{ is sent to the authorized users through a private channel.}$$

5.2.3 Index Encryption
Before hosting the encrypted records to the server, the
owner $o_i$ preprocesses data as the inverted index, where records can be retrieved by the keyword collection $W_i$. It
then defines the access policy tree $T_i$ for the searchable
keyword index and encrypts the index by running the
$IndEnc$ algorithm.

The algorithm takes the public parameter $pp$, public and
secret key $(pk_{o_i}, sk_{o_i})$, and access policy tree $T_i$ as input. To encrypt the owner level permission key, it chooses a random element $r_i \in Z_p^*$. It then generates the ciphertext of owner level
access permission of $o_i$ as
$$C_{i,ap} = (c_{i,1} = e(k_{i,1}^{r_i}, c_{i,2} = e(k_{i,2}^{r_i}, c_{i,3} = (v_{h_{i,2}})^{r_i})).$$ To encrypt the searchable keyword index with fine-grained
attribute level permission key, it first randomly chooses
$r_{i,1}, r_{i,2} \in Z_p^*$ and computes the ciphertext $W_{i,w}$ of keyword $w$ as
$$W_{i,w} = (W_{i,1} = g^{cr_{i,1}}, W_{i,2} = g^{br_{i,2}}, W_{i,3} = g^{a(r_{i,1}+r_{i,2})} g^{b(w_{r_{i,2}})}).$$ The algorithm then sets $r_{i,2}$ as the secret value that needs
to be protected by the access tree $T_i$. Secret shares of $r_{i,2}$ are distributed according to $T_i$ by random polynomials, and
the ciphertext of each leaf node $f$ associated with attribute
$att(f)$ is generated as
$$\forall f \in L(T_i) : W_f = g^{g_{f}(0)}, D_f = H_1(att(f))^{g_{f}(0)}.$$ The encrypted index of keyword $w$ is set as $I_{i,w} = (T_i, C_{i,ap}, W_{i,w}, \{W_{f, D_f}\}_{f \in C(T_i)})$. After encrypting all the
index, the owners uploads the ciphertexts to the server.

5.2.4 Trapdoor Generation
All the authorized users can query the interested keyword
$\tilde{w}$ by generating the search trapdoor by running $TdGen$
algorithm. Accordingly, the trapdoor consists of two parts, i.e., owner level permission trapdoor and attribute level
permitted keyword search token. The user $u$ first chooses random elements $x \in Z_p^*$ for given query keyword $\tilde{w}$. With
the owner level access permission key $sk_{u,ap}$ (in Eq. 1),
$u$ generates the corresponding trapdoors $Ap_{u,1}, Ap_{u,2}$ of owners and the server as
$$Ap_{u,1} = sk_{u,ap}u^x, Ap_{u,2} = pk_c^x.$$ The introduction of $Ap_{u,2}$ is to resist the keyword guessing
attack as mentioned earlier. For the access control in
attribute level, user $u$ chooses another random element
$s \in Z_p^*$. To match the encrypted keyword in the index, $u$
computes the encrypted token of query keyword $\tilde{w}$ as
$$Tk_{u,\tilde{w}} = (tok_1 = (g^s g^{bH_2(\tilde{w})})^s, tok_2 = g^{sc},$$
$$tok_3 = A^s = g^{(sc-rs)/b}).$$ To specify the authorization of its attribute, $u$ also needs to
generate the trapdoor for attributes accordingly with the attribute secret key $sk_{u,att}$ (shown in Eq. 2) as
$$Tk_{u,att} = (\forall at_j \in Atts : \{A_j = A_j^s, B_j = B_j^s\}).$$ User $u$ then uploads the secure trapdoor $Tp_{u,\tilde{w}} =$
$(Atts, S, (Ap_{u,1}, Ap_{u,2}), Tk_{u,\tilde{w}}, Tk_{u,att})$ to the server.

5.2.5 Multi-owner Multi-user Encrypted Search
Based on the encrypted indexes from owners and the secu-
cure trapdoors from users, the server performs the two-
level matches to find results by running $Search$ algorithm,
where both owner level and attribute level permissions are
satisfied as required by all owners.

(1) Owner Level Permission Verification
After receiving the trapdoor from user $u$, the server
first converts the owner level permission trapdoor $Ap_{u,1}$ (in
Eq. 6) into $Ap_i$ for each owner $o_i$ as
$$Ap_i = Ap_{u,1} \cdot \prod_{k \in S, k \neq i} h_{n+1-k+i,2}^{ver}.$$ where $S$ represents owners that give access permissions to
$u$, and $ver$ is the version number $VN$ from the authority.
Given the encrypted index of owner level permission $C_{i,ap}$
(as shown in Eq. 3) of $o_i$ and the trapdoor $Ap_{u,2}$ (in Eq. 6)
of $u$, the server then checks whether the dataset of current
$o_i$ is accessible to $u$ as
$$\frac{e(pub, c_{i,2})^{\beta_i} e(c_{i,2}, Ap_{u,2})}{e(Ap_i, c_{i,1})} = e(h_{n+1,2}^{ver}, c_{i,1}),$$ where $pub = \prod_{k \in S} h_{n+1-k+1,2}^{ver} = \prod_{k \in S} g_{n+1-k+1,2}$ and $h_{n+1,2}$ is the public key of owner $o_i$. If Eq. 10 holds, it shows
that $u$ is an authorized user to search the data of owner
$o_i$. Then, the server will continue the following fine-grained
attribute level match. Otherwise, the search result of owner
o_i is \emptyset for u. We can observe that the authorized set S is known to both users and the server in plaintext form. It seems that users can submit any illegal set that they want to the server for search. In our design, the aggregate key plays an important role. Only legal owners that are aggregated in owner level permission keys can pass the verification process. Thus, users can enjoy search services only when they submit a true authorized set.

Proof. Only the user who has the owner level permission aggregate key sk_u,ap can pass the verification process. We present the correctness of Eq. 10 as follows.

$$
eq \frac{e(\text{pub}, c_{1,3})^{\beta_1} \cdot e(c_{1,2}, A_{pu,2})}{e(A_{pu,1}, c_{1,1})} = \frac{e(\prod_{k \in S} g_{n+1-k}, (g^{\beta_2} g_{1,i}^{r_1})^{\beta_1 r_1}) \cdot e(g^{\beta_2 n_1 r_1}, g^{\beta_1 x})}{e(\prod_{k \in S} g_{n+1-k}, g^{\beta_2 x} \cdot \prod_{k \in S, k \neq i} g_{n+1-k,i}, g^{\beta_1 i r_1})}$$

$$= \frac{e(g_{n+1,i+1}, (g^{\beta_2 n_1 r_1})^{\gamma_{1,r_1}} g^{\beta_1 x}, g^{\beta_1 i r_1})}{e(g_{n+1,i+1} g^{\gamma_{1,r_1}}, g^{\beta_1 i r_1})} = e(h_{n+1,i+1}^{r_1}, h_{n+1,i+1}^{r_1}, c_{1,1}). \quad (11)$$

Here is an example to explain how owner level permissions are verified. As shown in Fig. 2, there are 3 owners in this system, and the authorized user u has access permissions of owner set S = \{1, 2\}. In this process, the server will perform computations accordingly receiving the trapdoor (A_{pu,1}, A_{pu,2}) from u. It needs to transform this trapdoor for access permission verification of each owner. For example, the server first generates parameters pub and A_{pu} for owner o_1. Then, it verifies the owner level permission of o_1 by checking Eq. 10. Here, it can be observed that owner o_1 can pass the verification for u. It is the same for owner o_2 since they are both accessible to u. However, the verification process will fail for owner o_3 due to the value of A_{pu}. This is because the set S and corresponding authorized aggregate key only contain o_1 and o_2.

Discussions: In AESM^2, the version number VN is given to the server. Another possible design is to embed VN into the public keys of owners, where the server will not know the version number. However, in this way, it is extremely time-consuming to update the public keys for each owner when the revocation happens in the owner level permission.

(2) Attribute Level Match

When the adjusted trapdoor A_{pu} of owner o_i can pass the owner level access permission verification (Eq. 10), the server will perform the attribute level match for the same trapdoor T_{pu,u} of the user u. Since each owner has its fine-grained policies on the keywords, the search results depend on the attributes that the user possesses. For the Atts in the trapdoor T_{pu,u}, the server first checks if there exists an attribute set Atts_x that satisfies the access policy tree T_i in encrypted index I_{w,i} of owner o_i. For at_j \in Atts_x, according to Eq. 5 and Eq. 8, the server will compute

$$E_f = e(A_j', W_f)/e(B_j', D_f) = e(g, g)^{r_{sq}^j(0)},$$

where att(f) = at_j for f \in L(T_i) (leaf node). The server then combines all the E_f based on T_i to recover the secret value E_{root} in a bottom-up fashion as E_{root} = e(g, g)^{r_{sq}^r(0)} = e(g, g)^{r_{sq}^r,2}.

With the encrypted index I_{w,i} (in Eq. 4) and trapdoor T_{pu,u} (in Eq. 7), the secret value E_{root} can be used to check whether the query keyword \hat{w} is matched as

$$e(W_{i,1}, tok_2) = e(W_{i,1}, tok_1) E_{root} e(tok_3, W_{i,2}). \quad (12)$$

If the query keyword \hat{w} exists in the encrypted index (i.e., \hat{w} = w), the Eq. 12 holds and it returns 1, which indicates that the server will return the corresponding records of queried keyword of owner o_i. Otherwise, it returns 0. The server needs to perform the attribute level match for each owner in the authorized set S of u in owner level permission, and then returns all the match records of owners.

5.3 Owner Level Permission Revocation in AESM^2

In multi-owner and multi-user distributed systems, the user’s access privileges may dynamically change. There are two requirements when the owner level permission revocation happens. First, the revoked users can only search with the new owner level permission set S'. It cannot search data from revoking owners even if it submits the trapdoor generated with the previous secret key to the server. Second, non-revoked users with the unchanged owner level
permission set $S$ can also search as before without affection. For example, a user $\hat{u}$ has access permissions from owner \{A, B, C\}. When the owner B revokes the permission for the user $\hat{u}$, $\hat{u}$ cannot get any data from owner B any longer. Other users with the access permission from owner B can continue accessing dataset of B as before.

Suppose an access permission $p_r$ is revoked for the user $\hat{u}$ by owner $o_r$. We use the term of Revoked Permission to denote permission $p_r$. The user $\hat{u}$ is denoted as the Revoked User. The revoked user’s permission set from owners is $S^*$ after revocation. We denote the users without owner level permission revocation as Non-revoked Users. The owner level permission revocation method includes three phases: Update Key Generation, Secret Key Update of Users, and System Version Number Update by Server.

5.3.1 Update Key Generation

When the permission $p_r$ of owner $o_r$ is revoked from a user $\hat{u}$, the authority will generate a new version number $V^* \neq \text{Ver}^*(\text{Ver}^* \neq \text{Ver})$. The authority generates a unique update key $UK_r$ by running the ApUKKey algorithm for non-revoked users and the server to update the version number of the system as

$$UK_r = \frac{\text{Ver}^*}{\text{Ver}}. \quad (13)$$

5.3.2 Secret Key Update of Users

The authority needs to run SKUpd algorithm to generate the latest version of secret keys for both revoked users and non-revoked users. It generates the new secret key for the revoked user (with permission set $S^*$) as

$$sk_{u,ap} = \prod_{k \in S^*} g_{n+1-k}^{\beta \cdot \text{Ver}^*}. $$

The authority transmits the new secret key $sk_{u,ap}$ and $S^*$ to the user $\hat{u}$ securely.

To avoid non-revoked users leaking the update key to the revoked user, the secret key update of non-revoked users is run by the authority (users do not get the update key). Based on the previous secret key ($sk_{u,ap}$ shown in Eq. 1), namely, there is no need for the authority to generate new keys for non-revoked users from scratch. It can generate the updated secret key for non-revoked users as

$$sk_{u,ap} = sk_{u,ap}^{UK_r}.$$  

The owner level permission sets are kept unchanged for non-revoked users. The authority will give each $sk_{u,ap}^{UK_r}$ to these non-revoked users through a private channel. All users will use the updated secret key to generate search trapdoors. The revocation function can be processed in batches according to time division, for example, every month. The authority will only be involved periodically after system initialization.

5.3.3 System Version Number Update by Server

To ensure that the revoked users cannot search with the previous secret key (before revocation), all the parameters (adapted trapdoors and search parameters) related to the owner level permission set are required to be updated to the latest version. The server conducts the update operation by using the proxy re-encryption method without decryption before updating. Because the index of each owner and the owner level permission set are decoupled in our design, we do not need to update the index ciphertexts generated by the owners, which greatly improves the update efficiency.

The server updates the system version number by running the algorithm VNUpd during search after owner level permission revocation. Upon receiving the update key $UK_r$ (in Eq. 13) from the authority, the server takes as inputs the trapdoors from the user associated with the owner level permission set and the update key $UK_r$ to update the converted trapdoor $Ap_i$ (in Eq. 9) for owner $o_i$ as

$$Ap_i^* = Ap_{u,1} \cdot \prod_{k \in S, k \neq i} h_{n+1-k+1,2}^{\text{Ver}^*}UK_r.$$  

The system parameters are also updated to the latest version during owner level permission verification (in Eq. 10) with the update key $UK_r$ as

$$\frac{e(\text{Pub}^*, c_{i,1})^{\beta_1} \cdot e(c_{i,2}, Ap_{u,2}) \cdot e(Ap_i^*, c_{i,1})}{e(Ap_i^*, c_{i,1})} \neq \frac{e(h_{n+1,2}^{\text{Ver}^*}, c_{i,1})}{e(h_{n+1,2}^{\text{Ver}^*}, c_{i,1})}UK_r.$$  

Discussions: In the two-level access control mechanism, the user’s revocation issues can also be divided into two levels. Here, we only focus on the flexible access revocation for users in the owner level permission. For the attribute level permission revocation, there are two kinds of update methods, i.e., access policy update and attribute revocation. Some excellent works [32], [39] have been proposed to cope with this problem. They can be easily integrated into the attribute level of AESM2.

6 Security Analysis

In this section, we first define the security model. Then, we formally prove the security of our protocol, which is selectively secure against CKA and achieves access control based search.

6.1 Security Model

Our protocol should achieve the selectively security against CKA (Chosen-Keyword Attack) for any PPT (Probabilistic Polynomial-Time) adversary. We formalize this security model by using the selective CKA game between an adversary $A$ and a challenger $C$.

- **Setup.** $A$ first chooses a non-trivial challenge $\mathcal{T}^*$ that can be satisfied by any user without valid attributes, then gives it to $C$ that will run Setup to output public parameters $pp$ and master key $msk$.

- **Phase 1.** $A$ issues the following oracles for polynomial times, and $C$ initializes an empty keyword list $\mathcal{L}_w$.

  - $O_{KeyGen}$. If the user’s attribute set $Atts$ satisfies the specified access tree $\mathcal{T}^*$, $C$ aborts. Otherwise, $C$ calls KeyGen and returns the secret key $sk_{u,att}$ for corresponding $Atts$.

  - $O_{TdGen}$. $C$ first calls TdGen to generate the trapdoor for $A$, then adds the keyword $w$ in $\mathcal{L}_w$ if the attribute set $Atts$ satisfies the access tree $\mathcal{T}^*$.

- **Challenge.** $A$ selects two challenging keywords $w_0, w_1 \notin \mathcal{L}_w$. $C$ first chooses a random bit $b \in \{0, 1\}$, then calls IndEnc to generate the index $I_{w_b}$ and sends it to $A$. It is
worth noticing that the requirement \(w_0, w_1 \notin L_w\) is to prevent \(A\) from trivially guessing the bit \(b\) based on the oracle \(O_{T_{dGen}}\).

- Phase 2. \(A\) repeats the process of Phase 1, but one limitation is that \(w_0, w_1\) cannot be queried to the oracle \(O_{T_{dGen}}\) if \(\text{Att} \cap \text{Set} \cap \text{OP}\) satisfies \(T^*\).
- Guess. \(A\) outputs a guess bit \(b'\) and wins the above game if \(b = b'\).

**Definition 1.** Let \(|Pr[b = b] - \frac{1}{2}|\) be \(A\)'s probability of winning above security game, and our protocol is selectively secure against CKA if \(|Pr[b = b] - \frac{1}{2}|\) is negligible in security parameter \(\lambda\).

In the public-key setting, it is difficult to prevent \(A\) from launching keyword guessing attack. \(A\) may first encrypt a keyword of its choice, and then check whether the resulting ciphertext and target trapdoor are derived from the same keyword. Thus, we form this security property as *keyword secrecy*, which requires that \(A\)'s probability in telling keyword ciphertext of its choice from target trapdoor is negligible. The keyword secrecy game simulated between adversary \(A\) and challenger \(C\) is demonstrated as follows.

- Setup. \(C\) calls \textbf{Setup} to generate the public parameters \(pp\) and master key \(msk\), then it sends \(pp\) to \(A\) and keeps \(msk\) itself.
- Phase 1. \(A\) makes polynomial time queries to the following oracles:
  - \(O_{KgGen}\). \(A\) submits an attribute set \(\text{Att}\) to \(C\). \(C\) calls \textbf{KeyGen} to return the corresponding secret key \(sk_{u, att}\) to \(A\). In addition, \(C\) adds \(\text{Att}\) into the list \(L_{att}\) which is initially empty.
  - \(O_{T_{dGen}}\). \(A\) submits a keyword \(w\) to \(C\). \(C\) calls \textbf{TdGen} to generate the trapdoor \(T_{pq,w}\) for \(A\).
- Challenge. \(A\) submits a non-trivial access policy \(T^*\) to \(C\). \(C\) first selects a keyword \(w^*\) and an attribute set \(\text{Att}^*\) that satisfies \(T^*\), then calls \textbf{IndEnc} and \textbf{TdGen} to output \(I_{i,w}, T_{pq,w}\), respectively. While the requirement is that \(\text{Att}^*\) does not satisfy \(T^*\) for any \(\text{Att} \in L_{att}\).
- Phase 2. This phase is similar to Phase 1.
- Guess. After guessing \(g\) different keywords, \(A\) outputs a keyword \(w'\). \(A\) wins this security game if \(w' = w\). Otherwise, it fails.

**Definition 2.** Our protocol can achieve the keyword secrecy if \(A\)'s advantage in winning above security game is at most \(\frac{1}{|W|} + \epsilon\), where \(|W|\) is the keyword space, and \(\epsilon\) is a negligible advantage.

### 6.2 Security Proof

**Theorem 1.** Our protocol is selectively secure against CKA in the generic bilinear group model [34], where \(H_1\) is modeled as a random oracle and \(H_2\) is a one-way hash function.

**Proof:** In the selective CKA game, the goal of \(A\) is to distinguish \(g^{\alpha(r_1+r_2)}b_{r,1}H_2(w_1)\) from \(g^{\alpha(r_1+r_2)}b_{r,1}H_2(w_0)\). Given a random element \(\theta \in Z^*_p\), the probability of distinguishing \(g^{\theta}\) from \(g^{\alpha(r_1+r_2)}g^{br_1,H_2(w_1)}\) is equal to that of distinguishing \(g^{\delta}\) from \(g^{\theta}\) for \(\delta \in Z^*_p\) and \(\alpha(r_1+r_2)\). Thus, \(A\) has an advantage \(\epsilon/2\) in distinguishing \(g^{\delta}\) from \(g^{\alpha(r_1+r_2)}g^{br_1,H_2(w_1)}\) if it can break the selective CKA game with an advantage \(\epsilon\). To prove above theorem, we consider a CKA game where \(A\) can distinguish \(g^{\alpha(r_1+r_2)}\) from \(g^{\delta}\), shown as follows.

- Setup. \(C\) selects three random elements \(a, b, c \in Z^*_p\) and returns partial public parameters \((e, g, p, g^a, g^b, g^c)\) to \(A\). Then, \(A\) chooses an access tree \(T^*\) and sends it to \(C\). \(H_{i}(at_{j})\) is simulated as follows. If the attribute \(at_j\) has been queried before, \(C\) chooses \(\pi_j \in Z^*_p\) and adds \((at_j, \pi_j)\) to \(O_{Hi}\) before returning \(g^{\pi_j}\). Otherwise, \(C\) returns \(g^{\pi_j}\) by using \(\pi_j\) in \(O_{Hi}\).
- Phase 1. \(A\) issues \(O_{KeyGen}, O_{TdGen}\) as follows.
  - \(O_{KeyGen}\). \(C\) chooses \(r \in Z^*_p\) and computes \(A = g^{\alpha(r-\gamma)/b}\). For each attribute \(at_j \in \text{Att}\), \(C\) first selects \(r_j \in Z^*_p\) and computes \(A_j = g^{\alpha_j}g^{\pi_jr_j}, B_j = g^{\gamma_j}\), then returns \((A, A_j, B_j)\).
  - \(O_{TdGen}\). \(C\) first issues the oracle \(O_{KeyGen}\) to get the secret key for attribute set \(\text{Att}\), then selects \(s \in Z^*_p\) and computes \(tok_1 = (g^sg^{bH_2(w)})^{\alpha}, tok_2 = g^{\pi_j}\), \(tok_3 = A^s, A_j^s = A_j^s, B_j^s = B_j^s\) for keyword \(w\). If \(\text{Att}\) satisfies \(T^*\), \(C\) stores \(w\) in \(L_w\).
- Challenge. Given two challenging keywords \(w_0, w_1 \notin L_w\) with the same length, \(C\) first chooses \(r_1, r_2 \in Z^*_p\) and computes the secret shares of \(r_{1,2}\) for leaf nodes in the specified access tree \(T^*\). Then, \(C\) selects a random bit \(b \in \{0, 1\}\) and computes \(W_0 = g^{\alpha r_1}, W_1 = g^{\alpha r_2}, W_3 = g^{\alpha r_1+r_2}, W_4 = g^{\alpha r_2}, D_1 = g^{\gamma r_1}, D_2 = g^{\gamma r_2}\). Otherwise, \(C\) returns \(W_1 = g^{\alpha r_1}, W_3 = g^{\alpha r_1+r_2}, W_4 = g^{\alpha r_2}, W_2 = g^{\alpha r_1}, D_1 = g^{\gamma r_1}, D_2 = g^{\gamma r_2}\).
- Phase 2. This phase has the same process as Phase 1 in the selective CKA game.
- Guess. Assume that \(A\) can construct \(e(g, g)^{\delta(a(r_1+r_2)/b)}\) for certain term \(g^\delta\) that can be constructed according to above oracle outputs, then it can utilize to distinguish \(g^\delta\) from \(g^{\alpha(r_1+r_2)}\). Thus, we still need to show that \(A\) can construct \(e(g, g)^{\delta(a(r_1+r_2)/b)}\) for certain term \(g^\delta\) with a negligible advantage. That is, \(A\) cannot break the selective CKA game with non-negligible advantage.

In the generic group model \((G, G_T)\), where \(G = \{\psi_0(x)|x \in Z_p\}, G_T = \{\psi_1(x)|x \in Z_p\}\), \(A\)'s advantage in guessing an element in the images of \(\psi_0\) and \(\psi_1\) is negligible. Next, we consider \(A\)'s probability in constructing \(e(g, g)^{\delta(a(r_1+r_2)/b)}\) from oracle outputs it has queried, where \(\delta \in Z^*_p\). Finally, let us consider how to construct \(e(g, g)^{\delta(a(r_1+r_2)/b)}\) for certain term \(\delta\). As the random element \(r_{1,1}\) only appears in the term \(cr_{1,1}\), the term \(\delta\) should contain \(c\) for constructing \(e(g, g)^{\delta(a(r_1+r_2)/b)}\). Assume that \(\delta = \delta'c\). \(A\) needs to construct \(\delta'acr_{1,2}\) by using terms \(br_{1,2}\) and \((ac - r)/b\). Due to \(br_{2,1}(ac - r)/b = acr_{1,2} - rr_{1,2}\), \(A\) should cancel \(rr_{1,2}\) according to terms \(\pi_j, r + \pi_jr_j\), \(q_f(0), q_f(\pi_j)\), where \(q_f(0)\) is the secret share of \(r_{1,2}\) according to the access tree \(T^*\). However, it is difficult to construct \(rr_{1,2}\) based on above terms, as \(rr_{1,2}\) can only be constructed on condition that the attributes corresponding to \(r_{j} + \pi_jr_j\) satisfies \(T^*\). Thus, we derive that \(A\) cannot gain a non-negligible advantage in above modified selective CKA game. That is, \(A\) just gains a negligible advantage in breaking the above selective CKA game. \(\Box\)

**Theorem 2.** Our protocol guarantees the keyword secrecy in the random oracle model, where \(H_2\) is a one-way hash function.

**Proof:** We construct a challenger \(C\) that simulates the
guessing the keyword

• \( C \) selects random elements \( a, b, c \in \mathbb{Z}_p^* \) and calls
  \textbf{Setup} to output the public parameters \( pp = (g, g^a, g^b, g^c, H_1, H_2) \) and master key \( msk \), where \( H_2 \) is a one-way hash function. Then, \( C \) simulates the random oracle \( |O_{H_2} (at_1)\) as the same way as Theorem 1.
  Specifically, if the attribute \( at_j \) has been queried before, \( C \) chooses \( \pi_j \in \mathbb{Z}_p^* \) and adds \( (at_j, \pi_j) \) to \( |O_{H_2}| \), before returning \( g^{\pi_j} \). Otherwise, \( C \) returns \( g^{\pi_j} \) by using \( \pi_j \) in \( |O_{H_2}| \). Finally, \( C \) sends \( pp \) to \( A \).

• \textbf{Phase 1}. \( A \) adaptively makes queries to the following oracles for polynomially-many times.
  \begin{itemize}
  \item \( |O_{KeyGen}|. \) \( A \) submits an attribute set \( Atts \) to \( C \). \( C \) calls \textbf{KeyGen} to generate the secret key \( sk_{u,att} \) to \( A \). Then, \( C \) adds \( Atts \) into the list \( L_{att} \) which is initially empty.
  \item \( |O_{TdGen}|. \) \( A \) submits the keyword \( w \) to \( C \). \( C \) calls \textbf{TdGen} to generate the trapdoor \( T_{p,u,w} \) by using the secret key \( sk_{u,att} \). Then, \( C \) sends \( T_{p,u,w} \) to \( A \).
  \end{itemize}

• \textbf{Challenge}. \( A \) submits an access policy tree \( T^*_p \) to \( C \). \( C \) firstly chooses an attribute set \( Atts^* \) that satisfies \( T^*_p \) and calls \textbf{KeyGen} to output the secret key \( sk_{u,att}^* \). Then, \( C \) randomly chooses a keyword \( w^* \) from the keyword space \( |W| \), and outputs the index \( i_{1,w^*} \) and trapdoor \( T_{p,u,w^*} \)

• \textbf{Phase 2}. This phase is similar to Phase 1.

• \textbf{Guess}. \( A \) guesses a keyword \( w^f \) and sends it to \( C \). \( C \) calls \textbf{IndEnc} to generate the index \( i_{1,w^f} \). If \( i_{1,w^f} \) matches with \( T_{p,u,w^*} \), \( A \) wins this secrecy game. Otherwise, \( A \) fails.

Assume that \( A \) has issued \( q \) different keywords before guessing the keyword \( w^f \), then the size of remaining keyword space is \( |W| - q \). In addition, as \( H_2(\cdot) \) is a one-way hash function, deriving \( w^* \) from the hash value \( H_2(w^*) \) is negligible. Thus, \( A \)'s advantage in winning the above secrecy game is at most \( \frac{1}{\log_2 q} + \epsilon \). That is, the probability of \( A \) in winning the above secrecy game is negligible. Therefore, our protocol guarantees the keyword secrecy in the random oracle model.

Our protocol not only prevents attackers (i.e., outsiders or honest-but-curious cloud server) deducing keyword secrecy from indexes but also disables them from launching keyword guessing attacks on trapdoors, even though they can obtain the secret key of cloud server.

**Theorem 3.** Our protocol can resist the keyword guessing attack from attackers on condition that CDH assumption holds.

\begin{proof}
We take the server as an example. When launching the keyword guessing attacks, the server can obtain the public parameters, its secret key \( sk_{c,ss} \) and submitted trapdoors. Suppose the server attempts to guess the keyword \( \hat{w} \) from trapdoor \( T_{p,u,w} \). Given the trapdoor components \( (Ap_{u,1}, Ap_{u,2}) = (sk_{u,ap} v^z, u^z) \), the server does the guessing attacks as follows.

• On input the public parameters \( u, u^r, v, \) the server wants to deduce \( v^r \) from the term \( sk_{u,ap} v^r \). For \( u, v \in G \), we set \( v = u^r \), where \( r \in \mathbb{Z}_p^* \). That is, given a tuple \( (u, v, v^z) \), the server attempts to deduce \( u^{rz_1} \).
  
  If the server can compute \( u^{rz_1} \), then it can deduce the authorized key \( sk_{u,ap} \) from multiple owners. The server then can obtain \( sk_{u,ap} \), which makes it successfully pass the owner level permission verification. However, The above case conflicts with the CDH assumption.

• If the server cannot deduce \( sk_{u,ap} \), then it does not have opportunity for attribute level matching. Even though it can pass the owner level permission verification, it still cannot pass the attribute level match verification if it does not have the attribute level permission key \( sk_{u,ap} \), which has proved by Theorem 1.

Thus, the cloud sever does not distinguish \( \hat{w} \) from those embedded in trapdoors, which means that it cannot have chance to successfully launching keyword guessing attack under the CDH assumption.

\end{proof}

**Theorem 4.** Our protocol guarantees confidentiality of owner level permission ciphertexts under the CDH assumption, which means that the unauthorized users cannot deduce any sensitive information from owner level permission ciphertexts.

\begin{proof}
Suppose the unauthorized users are attackers that may be curious to deduce the sensitive information from available ciphertext \( C_{i,ap} = (c_{i,1}, c_{i,2}, c_{i,3}) \), where \( c_{i,1} = g^{\beta_i x_{i,1}} \), \( c_{i,2} = g^{\beta_i x_{i,2}} \), \( c_{i,3} = g^{\gamma_i z_{i,3}} \). For ease of presentation, we define each unauthorized user as an attacker \( A \), then we simulate \( A \)'s attacks as follows.

- Given the ciphertexts \( (c_{i,1}, c_{i,2}, u, v, g^{\beta_i x_{i,1}}, g^{\gamma_i z_{i,3}}) \), the goal of \( A \) is to deduce \( g^{y_{i,3}} \). Due to \( u, v, g_i \in G \), we set \( v = u^{z_1}, g_i = u^{z_2} \), where \( z_1, z_2 \in \mathbb{Z}_p^* \). Then, \( A \) will use \( (u^{\gamma_i z_{i,1}}, u^{\gamma_i z_{i,1}}, u, u^{z_1}, u^{z_2}) \) to deduce \( u^{z_2 y_{i,3}} \). If \( A \) successfully deduces the term \( u^{z_2 y_{i,3}} \), then it can solve the CDH problem, which conflicts the CDH assumption.

- Given the ciphertext \( (c_{i,2}, c_{i,3}, u, v) \), the goal of \( A \) is to deduce the term \( v^{r_1} \). Let \( v = z_{i,1} \), where \( z \in \mathbb{Z}_p^* \), then \( A \) will use \( (z_{i,1}, z_{i,1}) \) to deduce \( z_{i,1}^{r_1} \). If \( A \) successfully deduces the term \( z_{i,1}^{r_1} \), it can break the CDH assumption.

Thus, \( A \) cannot deduce sensitive information from the available owner level permission ciphertexts under the CDH assumption. That is, our protocol can guarantee the confidentiality of owner level permission ciphertexts.

\end{proof}

**Theorem 5.** Our protocol also achieves controlled searching, which means that the users cannot access data out of the scopes of their privileges.

\begin{proof}
In our proof, the authorized users issue search queries over encrypted records owned by specified data owner set \( S \), but cannot search records outside this set. In addition, each user cannot generate the valid aggregate key for the new data owner set according to the known one. The proof of Theorem 5 is on the basis of following two lemmas.

\end{proof}

**Lemma 1.** Even though the honest-but-curious server colludes with a malicious user, the attacker still cannot issue search queries over encrypted records not in the scope of compromised aggregate key. In the Search algorithm, the at-
Table 3: Computational Cost Comparison

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>Ours</th>
<th>ASBKS [46]</th>
<th>ABDKS [47]</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyGen</td>
<td>$(m_g + n_j + 2)E + n_j H_1$</td>
<td>$(3n_a n_w + n_a + 1)E + n_a n_w H_1$</td>
<td>$(2n_j + 6)E$</td>
</tr>
<tr>
<td>IndEnc</td>
<td>$(7m + 2m_{ua})E + m_{ua} H_1$</td>
<td>$(2mn_{au} + 5m)E + m_{au} n_{we} H_1$</td>
<td>$(2mn_j + 8m)E + 2mE_T + mP$</td>
</tr>
<tr>
<td>TdGen</td>
<td>$(2n_j + 6)E$</td>
<td>$(2n_a n_v + n_a + 4)E$</td>
<td>$(2n_j + 4)E$</td>
</tr>
<tr>
<td>Search</td>
<td>$(2mn_S + m)E + (4m + 2mn_{aj} + 3m_S)P + mE_T$</td>
<td>$(2mn_a n_v + 4m)P$</td>
<td>$(2mn_j + 5m)P + 3mE_T$</td>
</tr>
</tbody>
</table>

Notes: 'm': number of owner, 'm_S': number of system attribute, 'n_a': number of possible values for each attribute, 'n_j': attribute number of user.

Table 4: Storage Cost Comparison

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>Ours</th>
<th>ASBKS [46]</th>
<th>ABDKS [47]</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyGen</td>
<td>$(2n_j + 2)</td>
<td>G</td>
<td>$</td>
</tr>
<tr>
<td>IndEnc</td>
<td>$(2mn_j + 6m)</td>
<td>G</td>
<td>$</td>
</tr>
<tr>
<td>TdGen</td>
<td>$(2n_j + 5)</td>
<td>G</td>
<td>$</td>
</tr>
<tr>
<td>Search</td>
<td>$3m</td>
<td>G</td>
<td>+ (4m + 2mn_S + 3m_S)</td>
</tr>
</tbody>
</table>

7 Implementation and Evaluation

7.1 Theoretical Evaluation

For theoretical evaluation, we will analyze our scheme (AEMS²) and the schemes ASBKS [46], ABDKS [47] from the computational cost (shown in Table 3) and storage cost (shown in Table 4). In computational cost analysis, we only consider the costly operations: modular exponentiation operation $E$ (or $E_T$) in group $G$ (or $G_T$), hash operation $H_1$, which maps the arbitrary strings into elements in group $G$ and pairing operation $P$. For the theoretical storage cost, we define the element length of $G$, $G_T$ and $Z_p$ as $|G|$, $|G_T|$ and $|Z_p|$, respectively.

From Table 3, we can find that the proposed AEMS² outperforms both ASBKS and ABDKS in KeyGen algorithm. This is because AESM² involves fewer modular exponentiation operations than those in ASBKS and ABDKS. In the execution of IndEnc algorithm, AESM² is more efficient than ASBKS since there are multiple transitional nodes in the access tree in ASBKS. Although our scheme AESM² has a higher computational cost than ABDKS, it does not bring much burden as this is a one-time computation. Comparing the costs of different schemes in TdGen process, we can easily learn that the performance of AESM² is similar to that of ABDKS, and both perform better than ASBKS when generating one trapdoor. However, when searching from multiple owners, both ASBKS and ABDKS need to iterate multiple times. The proposed AESM² is much more efficient, which can be revealed from the following experimental evaluation. In the Search algorithm, AESM² will be the most efficient when the owner level permission set number $m_S$ is much smaller than the number of owners $m$ in the system. All the computational operations in ASBKS and ABDKS are proportional to the owner’s number, while AESM² is affected more by the size of owner level permission set $m_S$.

In Table 4, we present the storage cost comparison of our scheme AESM² with ASBKS and ABDKS. In the KeyGen process, AESM² is approximately equal to the cost of ABDKS. Both schemes outperform the ASBKS since each attribute has multiple possible values in ASBKS scheme. In the process of IndEnc algorithm, the storage cost of the proposed AESM² is less than those in ASBKS and ABDKS.

2. For trapdoor, the storage cost is also the communication cost.
3. In this work, the element length in $G_T$ is the same as that in $G$.
4. We compare performances of schemes in users’ key generation.
When a user queries data from multiple owners, the storage cost of AESM² in TdGen is more efficient than those in ASBKS and ABDKS since AESM² aggregates multiple owners’ permissions into one trapdoor, which reveals the advantage of our design. In Search algorithm, the storage cost of AESM² is decided by the number of owner \( m \) and the size of permitted owner set \( m_S \), while the ASBKS and ABDKS schemes are both proportional to the number of owner \( n \). So, our scheme AESM² costs much less than those of the other two schemes when \( m_S \) is much smaller than \( m \). Thus, the proposed AESM² will be much storage-saving in the system with a large scale of owners.

### 7.2 Experimental Evaluation

To practically evaluate the performance, we simulate our scheme AESM² and other related works using the real-world dataset. The simulations are implemented in python on the Ubuntu server 18.04.3 with Intel Core i7-9700 CPU of 3.00GHz. We use the rapid cryptographic prototyping tool Crypto Charm [48] to implement the underlying operations. The bilinear pairing is initialized as Type A pairing by setting the symmetric curve SS512 in Charm. In our implementation, \( |G| = |G_T| = 1024 \text{ bits}, |\mathbb{Z}_p| = 160 \text{ bits.} \) We choose 10000 files and randomly extract 1000 keywords to test four main algorithms: KeyGen algorithm, IndEnc algorithm, TdGen algorithm, and Search algorithm in AESM² and related researches ASBKS and ABDKS scheme, respectively.

Fig. 3(a) and Fig. 3(b) show the performance of computational costs of three schemes in user key generation (KeyGen) with different number of owner and user's attribute, respectively. In Fig. 3(a), for comparison, we set the attribute number \( n_a = 10 \) in all three schemes. We can find that both the costs in ASBKS and ABDKS are proportional to the owner’s number when querying data from multiple owners. In contrast, the user key generation cost of our scheme AESM² is not influenced by the number of the owner. In Fig. 3(b), along with the different number of attribute of user, the cost of ABDKS is more efficient than those in AESM² and ASBKS since the additional hash operation \( H_1 \) is more time-consuming than exponentiation \( E \). For example, when setting \( n_j = 15 \), AESM² needs 75.85ms to generate keys, and ASBKS needs 142.09ms while ABDKS only costs 35.42ms. From Fig. 3(c), we can see that the time cost of owner key generation of AESM² increases when the number of the owner rises. In this stage, each owner generates their own public and secret key pairs, and this is a one-time cost. In owner level permission revocation, it is more efficient to update keys than to generate new keys for the users in AESM².

For IndEnc process, we also evaluate three schemes with regard to different number of the owner and the system attribute. Assuming the number of system attribute is \( n_a = 10 \) (the number of possible values \( n_v = 2 \) for each attribute in ASBKS) in Fig. 4(a), the time costs of index generation of three schemes are all proportional to the number of owners. As our scheme AESM² needs to encrypt the owner level permission and the keyword with attribute simultaneously, it takes extra \( 3mE \) exponentiation operations compared to the ABDKS scheme, while AESM² is still more efficient than the ASBKS scheme due to the consuming hash operation in ASBKS. For instance, setting the number of the owner \( m = 20 \), AESM² needs 61.10s to encrypt all 1000 keywords, while it takes 81.06s and 40.49s for ASBKS and ABDKS, respectively. Since the index generation algorithm is a one-time operation, it is acceptable for AESM² in practice. From Fig. 4(b), we can observe that all of the three schemes are not obviously influenced by the number of system attribute when the number of the owner is set to \( m = 10 \). This is because \( m \) will become the dominant factor with a large number of indexes in each owner. In AESM², the revocation of owner level permission will not influence the index generation phase (no re-encryption with the ciphertexts), which greatly reduces the system burden during revocation.

Fig. 4(c) demonstrates the efficiency of TdGen algorithm varying with different number of user’s attribute. The time cost is for one trapdoor generation. Our scheme AESM² is around the same cost as the ABDKS scheme, while both are less consuming than the ASBKS scheme. It is worth noting that AESM² is apparently much more efficient than the other two schemes when searching from multiple owners, as they both need to iterate multiple times. Practically, AESM² will bring a better search experience for the users. For example, setting \( m = 10, n_j = 10 \), AESM² consumes 26.25ms, while ASBKS and ABDKS individually need 359.5ms, 261.4ms.

In Fig. 4(d), we evaluate the computational efficiency of our scheme AESM² with regard to different number of the owner and the permitted number of owner level permission set \( S \). We can find that the number of the owner does
not have a big impact on the efficiency when the size of the permitted owner set \( m_S \) is constant. It is the \( m_S \) that plays a major role in the search process. Compared with the other two schemes, when the number of the owner in the system increases, the time consumption of AESM\(^2\) does not change much when the number in \( S \) is set to 10, as shown in Fig. 4(e). For instance, when \( m = 20, n = 20 \), the time costs of ASBKS and ABDKS increase from 40.50s to 121.20s, and 20.89s to 63.35s, respectively. Nevertheless, the cost of AESM\(^2\) remains almost unchanged, which varies from 15.98s to 16.45s. This advantage of AESM\(^2\) can be significantly efficient when there are many owners, and the permitted set \( S \) for the user is relatively small. The efficiency of Search algorithm is presented in Fig. 4(f), where the number of the owner is set to 20, and the size of \( S \) in AESM\(^2\) is 10. We can observe that the number of system attribute \( n_a \) does not influence much on all three schemes as the number of system attribute \( n_a \) remains the same. Fig. 5 analyzes the performance of TdGen and Search algorithms of three schemes for storage cost. We first evaluate the TdGen algorithm with different number of the owner in Fig. 5(a), where our scheme AESM\(^2\) is obviously more efficient than ASBKS and ABDKS. Both the other schemes need to generate a trapdoor for each owner, while AESM\(^2\) can query from multiple owners with one trapdoor submission. The storage overhead will not increase along with the owner's number the same as the other two schemes. For example, setting \( n_a = 10, n_v = 2, n_j = 10, \)
when $m$ doubles from 20 to 40, the storage overheads of ASBKs and ABDKS will change from 921600 bits to 1834200 bits, and 494720 bits to 989440 bits, while AESM$^2$ remains 25600 bits. This property of aggregate key greatly reduces the storage on the user side in our design. Accordingly, the communication overheads between the users and server of AESM$^2$ will be relatively smaller than the other schemes. In Fig. 5(b), when the number of the system owner increases, all the storage costs of Search process in three schemes will rise. In AESM$^2$, there is additional $3m|G|$ storage overhead in the owner level permission verification design. However, AESM$^2$ still performs more storage-saving than ASBKs and ABDKS. For instance, with $n_S = 10$, $n_u = 2$, $m_S = 10$, the cost of ASBKs is 921600 bits when the owner number $m$ is 20, and ABDKS needs 532480 bits space, while AESM$^2$ only costs 378880 bits. The system efficiency will benefit a lot from AESM$^2$ when there are many owners in the system with a relatively small permitted owner set. Moreover, we analyze the influence of the system attribute number in different schemes as shown in Fig. 5(c), where storage costs in all schemes rise when the number of system attribute increases. We can observe that our scheme AESM$^2$ brings less storage overhead than both ASBKs and ABDKS schemes. Thus, AESM$^2$ is desirable and efficient in the multi-owner and multi-user model.

8 Conclusion

In this paper, we study the data-sharing problem in multi-owner and multi-user distributed systems. We propose an efficient attribute-based encrypted keyword search scheme, named AESM$^2$, where access control requirements of owners are satisfied. Our design uses a two-level matching structure to achieve owner level permission and attribute level permission. In AESM$^2$, users can search data from multiple owners with a single search trapdoor. Furthermore, we design an efficient revocation method for users’ owner level permission. We formally prove the security of our scheme and also analyze the performance by comparing it with related works. Through theoretical and experimental comparison analysis, we show that our scheme AESM$^2$ is more efficient in terms of computation and storage costs in the multi-owner and multi-user model. A limitation of our work is the security assumption of the server. We rely on the server to perform efficient system updating for owner level permission revocation. So, it is necessary to assume that the server cannot help revoked users recover access permissions. Although our design is dynamic for access control, it can only support static databases. It is an interesting direction to design a cryptosystem that can achieve dynamic databases in the multi-owner and multi-user model.

Acknowledgements

This work was funded in part by National Natural Science Foundation of China under Grants 61732022, 62072361, and 62102035, Shenzhen Science and Technology Program under Grants GXWD20220817124827001 and JCYJ20210324132406016, Fundamental Research Funds for the Central Universities under Grant JB211105, the Research Grants Council of Hong Kong under Grants CityU 11213920, 11217819, 11217620, 11218521, 11202419, RF52122-1S04, C2004-21GF, R1012-21, and R6021-20F, and by InnoHK initiative, the Government of the HK SAR, and Laboratory for AI-Powered Financial Technologies.

References


Mingyue Wang received the B.E. degree in Computer Science from Harbin Engineering University in 2018. She is currently pursuing the Ph.D. degree in Department of Computer Science both with Harbin Institute of Technology, Shenzhen, and City University of Hong Kong. Her current research interests include cloud computing security, applied cryptography, and blockchain technology.

Yinbin Miao (M’18) received the B.E. degree with the Department of Telecommunication Engineering from Jilin University, Changchun, China, in 2011, and Ph.D. degree with the Department of Telecommunication Engineering from Xidian University, Xi’an, China, in 2016. He is also a postdoctor in Nanyang Technological University, and a postdoctor in City University of Hong Kong. He is currently an Associate Professor with the Department of Cyber Engineering in Xidian University, Xi’an, China. His research interests include information security and applied cryptography.

Yu Guo (M’19) is currently a Lecturer at the School of Artificial Intelligence, Beijing Normal University. He received his B.E. degree in Software Engineering from Northeastern University in 2013, the M.Sc degree in Electronic Commerce and Ph.D. degree in Computer Science from City University of Hong Kong in 2014 and 2019. He has also been a Postdoctor and Research Fellow at City University of Hong Kong. His research interests include cloud computing security, network security, privacy-preserving data processing, and blockchain technology.
Hejiao Huang graduated from the City University of Hong Kong and received the Ph.D. degree in computer science in 2004. She is currently a professor with the Department of Computer Science in Harbin Institute of Technology (Shenzhen), Shenzhen, China, and previously was an invited professor at INRIA, France. Her research interests include cloud computing, trustworthy computing, formal methods for system design and wireless networks.

Cong Wang (F'21) is currently a Professor in the Department of Computer Science, City University of Hong Kong. His research interests include data and network security, blockchain and decentralized applications, and privacy-enhancing technologies. He has been one of the Founding Members of the Young Academy of Sciences of Hong Kong since 2017, and has been conferred the RGC Research Fellow in 2021. He is a co-recipient of the Best Paper Award of IEEE ICDCS 2020, ICPADS 2018, MSN 2015, the Best Student Paper Award of IEEE ICDCS 2017, and the IEEE INFOCOM Test of Time Paper Award 2020. His research has been supported by multiple government research fund agencies, including National Natural Science Foundation of China, Hong Kong Research Grants Council, and Hong Kong Innovation and Technology Commission. He has served as associate editor for IEEE TDSC, IEEE TSC, IEEE IoT-J, IEEE Networking Letters, and The Journal of Blockchain Research, and TPC co-chairs for a number of IEEE conferences and workshops. He is a fellow of the IEEE, and member of the ACM.

Xiaohua Jia (F'13) received the BSc and MEng degrees in 1984 and 1987, respectively, from the University of Science and Technology of China, and the DSc degree in 1991 in information science from the University of Tokyo. He is an adjunct in Harbin Institute of Technology (Shenzhen) while performing this work. He is currently the chair professor with the Department of Computer Science at City University of Hong Kong. His research interests include cloud computing and distributed systems, computer networks, wireless sensor networks and mobile wireless networks. He is an editor of the IEEE TPDS (2006-2009), Wireless Networks, Journal of World Wide Web, Journal of Combinatorial Optimization, etc. He is the general chair of ACM MobilHoc 2008, TPC co-chair of IEEE MASS 2009, area-chair of IEEE INFOCOM 2010, TPC co-chair of IEEE GlobeCom 2010-Ad Hoc and Sensor Networking Symposium, and Panel co-chair of IEEE INFOCOM 2011. He is fellow of the IEEE Computer Society.