Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing

NARESH NAIDU, R1, G. SPANDANA2, B. HARI KRISHNA3

1PG Scholar, Dept of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, TS, India, E-mail: nareshnaidu.rangineni@gmail.com.
2Assistant Professor, Dept of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, TS, India, E-mail: spandanasar@gmail.com.
3HOD, Dept of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, TS, India, E-mail: hariboorgadda@gmail.com.

Abstract: With the growing popularity of cloud computing, organizations and data owners starts to outsource their important data to the public cloud for reduced management cost and ease of access. Encryption helps to protect user data confidentiality, it makes difficult to perform secure plain text search over the encrypted data. In this paper, we present some combination between verifiable computation and encrypthen-Mac mechanism. To support the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time security against chosen plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. The result gives more feasible and efficiency of the proposed solution.

Keywords: Ciphertext-Policy Attribute-Based Encryption, Circuits, Verifiable Delegation, Multi-Linear Map, Hybrid Encryption.

I. INTRODUCTION

Cloud computing is the computing technique which describes the combination of logical entities like data, software which are accessible via internet. Cloud computing provides help to the business applications and functionality along with the usage of computer software by providing remote server which access through the internet. Client data is generally stored in servers spread across the globe. Cloud computing allows user to use different services which saves money that users spend on applications. Data owners and organizations are motivated to outsource more and more sensitive information into the cloud servers, such as emails, personal documents, videos and photos, company finance data, government documents, etc. To provide end-to-end data security and privacy in the cloud, sensitive data has to be encrypted before outsourcing to protect data privacy. In cloud computing, effective data utilization is a very difficult task because of data encryption, also it may contain large amount of outsourced data files. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user’s demands.

To overcome the above problem in this paper new technique is introduced technique which used Cipher text policy attribute-based encryption. In this scheme is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. Some problem of applying the only attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. So we used the cipher text –policy attribute encryption. As applications move to cloud computing platforms, cipher text-policy attribute-based encryption (CPABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. Data owners may wants to share their outsourced data with other large amount of users. Users may want to only retrieve certain specific data files they are interested in during a given session. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. They focused on policies across multiple authorities and the issue of what expressions they could achieve. Uses another form of encryption is hybrid encryption for encrypt messages of arbitrary length a onetime MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Attribute-based encryption with verifiable delegation is decryption scheme to reduce the computation cost during decryption.

II. PROBLEM STATEMENT

A. Securely Outsourcing Attribute-Based Encryption with Check Ability

In this paper, Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. We propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption.
B. Privacy-Preserving Decentralized Key-Policy Attribute Based Encryption

In this paper, they have proposed privacy-preserving decentralized key-policy ABE scheme where each authority can issue secret keys to a user independently without knowing anything about his GID. Therefore, even if multiple authorities are corrupted, they cannot collect the user’s attributes by tracing his GID.

C. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems

In this paper, we propose an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group.

D. Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization

In this paper, we proposed new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encrypt or to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model.

E. Decentralizing Attribute-Based Encryption

In paper, we propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority.

F. Universally Composable Secure Channel Based on the KEM-DEM Framework

In paper, For ISO standards on public-key encryption, Show up introduced the framework of KEM (Key Encapsulation Mechanism), and DEM (Data Encapsulation Mechanism), for formalizing and realizing one-directional hybrid encryption; KEM is a formalization of asymmetric encryption specified for key distribution, and DEM is a formalization of symmetric encryption. This paper investigates a more general hybrid protocol, secure channel, using KEM and DEM, such that KEM is used for distribution of a session key and DEM, along with the session key, is used for multiple bi-directional encrypted transactions in a session. This paper shows that KEM semantically secure against adaptively chosen ciphertext attacks (IND-CCA2) and DEM semantically secure against adaptively chosen plaintext/ciphertext attacks (IND-

III. EXISTING AND PROPOSED SYSTEMS

A. Existing System

The servers could be used to handle and calculate numerous data according to the user’s demands. As applications move to cloud computing platforms, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. The increasing volumes of medical images and medical records, the healthcare organizations put a large amount of data in the cloud for reducing data storage costs and supporting medical cooperation. There are two complementary forms of attribute based encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE).

Disadvantages of Existing System:

- The cloud server might tamper or replace the data owner’s original ciphertext for malicious attacks, and then respond a false transformed ciphertext.
- The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible.

B. Proposed System

We firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. The proposed scheme is proven to be secured based on k-multi-linear Decisional Diffie-Hellman assumption as shown in Fig.1. On the other hand, we implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly.

Disadvantages of Existing System:
- The cloud server might tamper or replace the data owner’s original ciphertext for malicious attacks, and then respond a false transformed ciphertext.
- The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible.

Proposed System

We firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. The proposed scheme is proven to be secured based on k-multi-linear Decisional Diffie-Hellman assumption as shown in Fig.1. On the other hand, we implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed ciphertext to help him/her decrypt the ciphertext immediately and correctly.
Advantages of Proposed System:

- The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
- They seek to guarantee the correctness of the original ciphertext by using a commitment.
- We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CPABE is conceptually closer to the traditional access control methods.

IV. IMPLEMENTATION

In this section, we simulate the cryptographic operations by using of the GNU MP library in v6.0. The experiments are performed on a computer using the Intel Core i5-2400 at a frequency of 3.10 GHz with 4GB memory and Windows 7 operation system. Without considering the addition of two elements over the integer, the hash function and exclusive-OR operations, we denote the cost of a multi-linear pairing by \( P \). \( \lambda \) denotes the security parameter. \( B \) denotes the group elements size in bits. With different parameters, the average running time of \( P \) operation in 100 times is obtained and demonstrated in TABLE 1. For \( P \) operations, in order to implement in practice efficiently, we use the optimized definition. We instantiate our hybrid VD-CPABE scheme with \( \lambda = 80 \) and \( \beta = 160 \). When we operate the encryption and partial decryption algorithms, the input wire and the AND gate need to garble twice and the OR gate needs to garble triple. The algorithm for generating MAC needs one garbling operation and other addition operations over the integer, and the algorithm for verifying MAC needs to garble triple. Based on the above parameter settings, the most running time to finish our encryption and decryption algorithms are illustrated in Fig. 2.

![Performance of our hybrid VD-CPABE scheme.](image)

In addition, suppose that the symmetric cipher is 128-bit. The bandwidth of the transmitted ciphertext for the data owner grows with the increase of the depths of circuit. For the user, the bandwidth of the transmitted ciphertext is \((128 \times 2 + 160 \times 3)/8 = 92\) bytes. Obviously, for the data owner and the cloud server, the computation time grows exponentially with the increase of the depth of circuit. When depth(C) = 1, these computation are 96ms and 0ms, respectively. While the cost of computation consumption at the user side is just 64ms which is independent of the depth of the circuit thus our scheme enables to provide an efficient method to share and protect the confidential information between users with limited power and data owners with vast amount of data in the cloud. In this paper, we firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-Mac mechanism with our ciphertext policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

**TABLE I: Pairing Operation Time**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>( \lambda )</th>
<th>( \beta )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \lambda = 62 )</td>
<td>( \lambda = 80 )</td>
<td>( \lambda = 160 )</td>
</tr>
<tr>
<td>( \beta = 80 )</td>
<td>( \beta = 160 )</td>
<td>( \beta = 200 )</td>
</tr>
<tr>
<td>Time</td>
<td>15ms</td>
<td>16ms</td>
</tr>
</tbody>
</table>

V. CONCLUSION

To the best of our knowledge, we firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext-policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to the cloud server. In addition, the proposed scheme is proven to be secure based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.
consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

VI. REFERENCES


