A Secure Circuit Ciphertext-Policy Attribute-Based Encryption In Cloud Computing

Vishal Pachangane  
Department of Computer Engineering  
Alard College Of Engineering And Management  
Pachangane.vishal@gmail.com

Prof. Priti Gode  
Department of Computer Engineering  
Alard College Of Engineering And Management  
godepriti@gmail.com

Abstract—In the cloud, for accomplishing access control and data security, the data owners could use attribute-based encryption to encrypt the stored data. To reduce the cost, the users which have a limited computing power are nevertheless more likely to delegate the task of the decryption power to the cloud servers. The result shows, attribute-based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated ciphertext and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been developed. This system is mixed with verifiable computation and encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. As well as this scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, this scheme achieves feasibility as well as efficiency.

Index Terms—Ciphertext-policy attribute-based encryption, circuits ,hybrid encryption, multi linear map, verifiable delegation.

I. INTRODUCTION

Cloud computing is innovation which uses advanced computational power as well as improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the users burden. As applications shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping. To make such data sharing be achievable, attribute based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each ciphertext is contains an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the keys attribute set satisfies the access structure associated with a ciphertext. The cloud server provides another service which is delegation computing. The VD-CPABE scheme shows that the untrusted cloud will not be able to learn anything about the encrypted message and build the original ciphertext.

II. REVIEW OF LITERATURE

1) Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems [1].The author proposes 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.

2) Privacy-preserving decentralized key-policy attribute-based Encryption [2]. The author propose a 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. Notably, our scheme only requires standard complexity assumptions (e.g., decisional bilinear Diffie-Hellman) and does not require any cooperation between the multiple authorities, in contrast to the previous comparable scheme that requires nonstandard complexity assump-
3) Practical Multilinear Maps over the Integers [3]. The author describes a different construction that works over the integers instead of ideal lattices, similar to the DGHTV fully homomorphic encryption scheme. He also describes a different technique for proving the full randomization of encodings: instead of Gaussian linear sums, and apply the classical leftover hash lemma over a quotient lattice. We show that our construction is relatively practical: for reasonable security parameters a one-round 7-party Diffie-Hellman key exchange requires less than 40 seconds per party.

4) A new paradigm of hybrid encryption scheme [4]. The author shows that a key encapsulation mechanism (KEM) does not have to be IND-CCA secure in the construction of hybrid encryption schemes, as was previously believed. That is, we present a more efficient hybrid encryption scheme than Shoup [12] by using a KEM which is not necessarily IND-CCA secure. Nevertheless, our scheme is secure in the sense of IND-CCA under the DDH assumption in the standard model.

5) A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack [5]. A new public key cryptosystem is proposed and analyzed. The scheme is quite practical, and is provably secure against adaptive chosen ciphertext attack under standard intractability assumptions. There appears to be no previous cryptosystem in the literature that enjoys both of these properties simultaneously.

6) Attribute-based encryption with verifiable outsourced decryption [6]. The author first formalizes a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. Then, he presents an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourcing decryption. The new approach is simple, general, and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user’s and the cloud server’s computation costs except some non-dominant operations (e.g., hash computations), nor expands the ciphertext size except adding a hash value (which is 20 byte for 80-bit security level).

7) Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [7]. The author presents a new methodology for realizing Ciphertext-Policy Attribute Encryption (CPABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. The author presents three constructions within this framework. The first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. The next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

8) Decentralizing attribute-based encryption [8]. The author proposes a Multi-Authority Attribute-Based Encryption (ABE) system. In this 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.

9) How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption [9]. In this work the author extends the definition of verifiable computation in two important directions: public delegation and public verifiability, which have important applications in many practical delegation scenarios. Yet, existing VC constructions based on standard cryptographic assumptions fail to achieve these properties.

10) Outsourcing the decryption of ABE Ciphertexts [10]. The author proposes a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE ciphertexts are stored in the cloud. We show how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user’s attributes into a (constant-size) El-Gamal-style ciphertext, without the cloud being able to read any part of the user’s messages.

III. SYSTEM ARCHITECTURE

The system contains four modules,
1. Cloud Storage Module
2. Data Owner Module
3. Data User Module
4. Authority Module

Cloud Storage: Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data. Data Owner: The data owner encrypts his message under access policy, then computes the complement circuit, which outputs the opposite bit of the output of f, and encrypts a random element R of the same length to under the policy Data User: The users can outsource their complex access control policy decision and part process of decryption to the cloud. Which extended encryption ensures that the users can obtain either the message M or the random element R, which avoids the scenario when the cloud server deceives the users that they are not satisfied to the access policy, however, they meet the access policy actually.

Authority: Authority generates private keys for the data owner and user.

ADVANTAGES:
- The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
- Gives guarantee for correctness of the original ciphertext by using a commitment.
- Achieve security, confidentiality and access control.

IV. MATHEMATICAL MODELING

\[ S = s, e, X, Y, \phi \]

\( S = \) Set of system

\( s = \) Start of the program

Register to system.

Login to system.

\( X = \) Input of the program

\( X = F, A1, A2, \ldots, An, AC \)

Where,

\( F = \) File uploaded by Owner.

\( A1, A2, \ldots, An = \) Attributes set to file by Owner.

\( AC = \) Access policy generated by Owner

\( Y = \) Output of the program

\( Y = RD \)

\( RD = \) Retrieved file after decryption from storage system.

User can download the file if any only if attributes and access policy user are matching with attributes and access policy of file given by owner.

\( e = \) End of the program

\( \phi = \) Success or failure condition of system

Above mathematical model is NP-Complete.

V. RESULTS

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 \((128*2+160*3)/8=92\) 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 computations are 96 ms and 0 ms, respectively. While the cost of computation consumption at the user side is just 64 ms 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.
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.

VI. CONCLUSION

Design a circuit ciphertext-policy attribute-based hybrid encryption with provable allocation method. The universal circuits are helpful to achieve or clear the strongest form of entre manage strategy. Collective provable calculation and encrypt-then-Mac system with our ciphertext policy attribute-based hybrid encryption, we could assign the provable fractional decryption paradigm to the cloud server. The k-multilinear Decisional Diffie-Hellman assumption proves the proposed scheme is secure. On the other side, this scheme can use over the integers. The conclusion show that the method is sensible in the cloud computing. Thus, can be able to achieve data privacy, the fine-grained entre manages and the demonstrable allocation in cloud.

REFERENCES