Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute Based Encryption

D. HARICHRAN REDDY¹, K. SRINIVAS²

¹PG Scholar, Dept of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, TS, India,
Email: haricharan.reddy12@gmail.com.
²Associate Professor, Dept of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, TS, India.

Abstract: Cloud computing is a revolutionary computing environment, which allows user a flexible, on-demand, and low-cost usage of computing resources, but as the data is outsourced to some cloud servers, and various privacy issues emerge from it. To handle these security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. Attribute-based Encryption (ABE) is a cryptographic conducting tool to guarantee data owner’s direct control over their data in public cloud storage. ABE is an encryption method used by the user to store the data in the cloud. ABE is a public-key based one to many encryption methodologies which allows users to encrypt and decrypt data based on user attributes. In this paper we studied various schemes of ABE like KP-ABE, CP-ABE, Anony Control and Anony Control-F, also we analyzed how data access privilege and data sharing can be controlled by using various schemes of ABE.

Keywords: Anonymity, Multi-Authority, Attribute-Based Encryption.

I. INTRODUCTION

Cloud computing is a revolutionary computing technique, by which computing resources are provided dynamically via Internet and the data storage and computation are outsourced to someone or some party in a cloud. In cloud storage systems, there are multiple authorities co-exist and each authority is able to issue attributes independently. Cloud computing provides a scalable, location-independent and high performance solution by delegating computation tasks and storage into the resource-rich clouds. This overcomes the resource limitation of users with respect to data storage, data sharing and computation various techniques have been proposed to protect the data contents privacy via access control Identity-based encryption (IBE) [4,7,12,14,15], Fuzzy Identity-Based Encryption Key-Policy Attribute-Based Encryption (KP-ABE) [5,6,10], Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [3,8,11,13] and AnonyControl and AnonyControl-F [1] to allow cloud servers to control user’s access privileges without knowing their identity information. In the KP-ABE, a cipher text is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user’s identity (e.g. IIT AND (Ph.D OR Master)). A user can decrypt the cipher text if and only if the access tree in his private key is satisfied by the attributes in the cipher text. However, the encryption policy is described in the keys, so the encrypted does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

On the other hand, those problems and overhead are all solved in the CP-ABE. In the CP-ABE, cipher texts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users’ attributes. A user can decrypt the cipher text if and only if his attributes in the private key satisfy the access tree specified in the cipher text. By doing so, the encrypted holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots. Unlike the data confidentiality, less effort is paid to protect users’ identity privacy during those interactive protocols. Users’ identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. But it seems natural that users are willing to keep their identities secret while they still get their private keys. Therefore Anony Control and Anony Control-F [1] to allow cloud servers to control users’ access privileges without knowing their identity information. The schemes are able to protect user’s privacy against each single authority. Partial information is disclosed in Anony Control and no information is disclosed in Anony Control-F. The schemes are tolerant against authority compromise, and compromising of up to (N − 2) authorities does not bring the whole system down.

II. EXISTING AND PROPOSED SYSTEMS

A. Existing System

Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy
Identity-Based Encryption is proposed, which is also known as Attribute-Based Encryption (ABE). The work by Lewko et al. and Muller et al. are the most similar ones to ours in that they also tried to decentralize the central authority in the CP-ABE into multiple ones. Lewko et al. use a LSSS matrix as an access structure, but their scheme only converts the AND, OR gates to the LSSS matrix, which limits their encryption policy to Boolean formula, while we inherit the flexibility of the access tree having threshold gates. Muller et al. also supports only Disjunctive Normal Form (DNF) in their encryption policy.

B. Proposed System

The data confidentiality, less effort is paid to protect users’ identity privacy during those interactive protocols. Users’ identities, which are described with their attributes, are generally disclosed to key issuers, and the issuers issue private keys according to their attributes. We propose AnonyControl and AnonyControl-Fallow cloud servers to control users’ access privileges without knowing their identity information. In this setting, each authority knows only a part of any user’s attributes, which are not enough to figure out the user’s identity. The scheme proposed by Chase et al. considered the basic threshold-based KP-ABE as shown in Fig.1. Many attribute-based encryption schemes having multiple authorities have been proposed afterwards. In our system, there are four types of entities: N Attribute Authorities (denoted as A), Cloud Server, Data Owners and Data Consumers. A user can be a Data Owner and a Data Consumer simultaneously. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users’ personally identifiable information.

III. MODULE DESCRIPTION

A. Number of Modules

After careful analysis the system has been identified to have the following modules:

- Registration based Social Authentication Module
- Security Module
- Attribute-based encryption module.
- Multi-authority module.

1. Registration-Based Social Authentication Module: The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password), and then a few (e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s Registration.

2. Security Module: Authentication is essential for securing your account and preventing spoofed messages from damaging your online reputation. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. Trustee-based social authentication systems ask users to select their own trustees without any constraint. In our experiments (i.e., Section VII), we show that the service provider can constrain trustee selections via imposing that no users are selected as trustees by too many other users, which can achieve better security guarantees.

3. Attribute-based Encryption Module: Attribute-based encryption module is using for each and every node encrypt data store. After encrypted data and again the re-encrypted the same data is using for fine-grain concept using user data uploaded. The attribute-based encryptions have been proposed to secure the cloud storage. Attribute-Based Encryption (ABE) in such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a descriptor’s identity has some overlaps with the one specified in the ciphertext.

4. Multi-authority Module: A multi-authority system is presented in which each user has an id and they can interact with each key generator (authority) using different pseudonyms. Our goal is to achieve a multi-authority CP-ABE which achieves the security defined above; guarantees the confidentiality of Data Consumers’ identity information; and tolerates compromise attacks on the authorities or the...
Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption

collusion attacks by the authorities. This is the first implementation of a multi-authority attribute based encryption scheme.

IV. PERFORMANCE EVALUATION

In this section, we present the performance evaluation based on our measurement on the implemented prototype system of AnonyControl-F. To the best of our knowledge, this is the first implementation of a multi-authority attribute based encryption scheme. Our prototype system provides five command line tools.

- **anonycontrol-setup**: Jointly generates a public key and N master keys.
- **anonycontrol-keygen**: Generates a part of private key for the attribute set it is responsible for.
- **anonycontrol-enc**: Encrypts a file under r privilege trees.
- **anonycontrol-dec**: Decrypts a file if possible.
- **anonycontrol-rec**: Decrypts a file and re-encrypts it under different privilege trees.

![Fig2. Experiment result on our implemented prototype system. (a) Setup time. (b) Keygen time with different authority’s #. 20 attributes per key. (c) Keygen time with different attributes #. 4 authorities. (d) Encryption and decryption time with different attributes number. File size is 100KB. (e) Encryption and decryption time with different file size. 20 attributes in T<sub>0</sub>. (f) Time to create a privilege tree and decrypt a verification parameter from it.](image)

This toolkit is based on the CP-ABE toolkit [5] which is available online, and the whole system is implemented on a Linux system with Intel i7 2nd Gen @ 2.7GHz and 2GB RAM. Fig. 2 shows the computation overhead incurred in the core algorithms Setup, Key Generate, Encrypt, and Decrypt under various conditions. We additionally implemented three similar works (Li, Chase, and Müller) under the same condition (same security level and same environment) for the comparison purpose. Particularly, in Fig. 2(e), we set only one privilege for the file access, and we measured the time to create one privilege tree and calculate its verification parameter in Fig. 2(f). In general, the computation overhead of Li, is much higher than others because their scheme involves many more exponentiations and bilinear mappings due to the accountability. The encryption/decryption under different file sizes did not show big differences when file sizes are large (≥20MB), because the run times are dominated by the symmetric encryption (AES-256). Finally, only our run times are plotted in Fig. 2(f) because the privilege creation is the unique process in our scheme.

V. CONCLUSION

In this paper, the survey of different encryption scheme like IBE, ABE, KP-ABE, CP-ABE, Anony control and Anony Control-F is mentioned with their advantage and disadvantage. The different variation of this scheme are compared and discussed with the existing scheme according to the rise in the security issues in cloud computing. The comparisons and study of those encryption scheme are done according to the problems arises and the solution on those the problem are mentioned. Direction for future work is to allow multi authority servers to update user secret key without disclosing user attribute information. Also in Anony Control system we worked with multi authority system, so it will be interesting to work with load balancing techniques to handle overhead.

VI. REFERENCES


Author’s Profile:

Haricharan Reddy, D, CSE Dept in Avanthi Institute of Engineering & Technology, Hyderabad, India, Email ID: haricharan.reddy12@gmail.com.

Mr. K. Srinivas, Assoc Prof, He has done his B.Tech in Computer Science and Engineering from JNTU Hyderabad, and completed his M.Tech in CSE from JNTU Hyderabad. His areas of interests are Network Security and Cryptography, Web-Technology and Compiler Design. At present, he is working as Assoc. Professor of CSE Dept in Avanthi Institute of Engineering & Technology, Hyderabad, Andhra Pradesh, India.