ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

M.S.Nirmal Kumar
Assistant Professor
Princeton College of Engineering and Technology,
Hyderabad.

Abstract:
Cloud computing is a revolutionary computing paradigm, which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. However, most work focuses on the data contents privacy and the access control, while less attention is paid to the privilege control and the identity privacy. In this paper, we present a semi-anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Subsequently, we present the AnonyControl-F, which fully prevents the identity leakage and achieve the full anonymity. Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes.

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'. It greatly attracts attention and interest from both academia and industry due to the profitability, but it also has at least three challenges that must be handled before coming to our real life to the best of our knowledge. First of all, data confidentiality should be guaranteed. The data privacy is not only about the data contents. Since the most attractive part of the cloud computing is the computation outsourcing, it is far beyond enough to just conduct an access control. More likely, users want to control the privileges of data manipulation over other users or cloud servers. This is because when sensitive information or computation is outsourced to the cloud servers or another user, which is out of users' control in most cases, privacy risks would rise dramatically because the servers might illegally inspect users' data and access sensitive information, or other users might be able to infer sensitive information from the outsourced computation. Therefore, not only the access but also the operation should be controlled. Secondly, personal information (defined by each user's attributes set) is at risk because one's identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).

As people are becoming more concerned about their identity privacy these days, the identity privacy also needs to be protected before the cloud enters our life. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. Various techniques have been proposed to protect the data contents privacy via access control. Identity-based encryption (IBE) was first introduced by Shamir [1], 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,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Fuzzy Identity-Based Encryption [2] is proposed, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes, and decryption is possible if a decrypter's identity has some overlaps with the one specified in the ciphertext. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) [3] and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [4], are presented to express more general condition than simple 'overlap'. They are counterparts to each other in the sense that the decision of encryption policy (who can or cannot decrypt the message) is made by different parties. In the KP-ABE [3], a ciphertext 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 ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encryption policy is described in the keys, so the encrypter 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 [4].

In the CP-ABE, ciphertexts 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 ciphertext if and only if his attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encrypter 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, we propose AnonyControl and AnonyControl-F (Fig. 1) to allow cloud servers to control users' access privileges without knowing their identity information. Their main merits are:

- The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F.
- The proposed schemes are tolerant against authority compromise, and compromising of up to $(N - 2)$ authorities does not bring the whole system down. 3) We provide detailed analysis on security and performance to show feasibility of the scheme AnonyControl and AnonyControl-F.
- We firstly implement the real toolkit of a multi-authority based encryption scheme AnonyControl and AnonyControl-F.

EXISTING SYSTEM:

The user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semianonymity. Besides, it also generalizes the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Extend existing schemes by generalizing the access tree to a privilege tree. The privilege in our scheme is defined as similar to the privileges managed in ordinary operating systems.

DISADVANTAGE FOR EXISTING SYSTEM:

1) Anony Control decentralizes the central authority to limit the identity leakage and thus achieves semianonymity

2) The privilege is not possible scheme is defined as similar to the privileges managed in ordinary operating systems

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

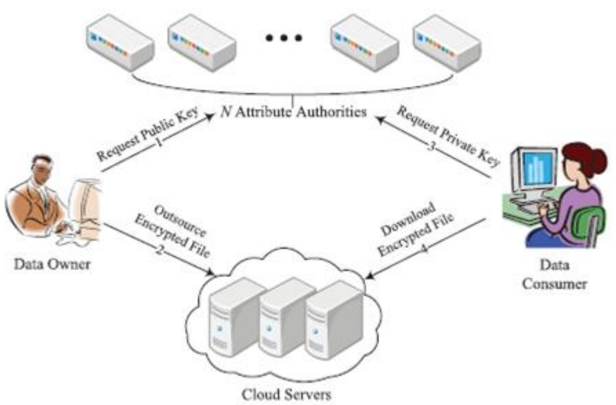
PROPOSED SYSTEM:

Our security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption, and our performance evaluation exhibits the feasibility of our schemes. In the proposed scheme, an authority generates a set of random secret parameters and shares gskj it with other authorities via secure channel, and is computed based on this parameters. It is believed that DDH problem is intractable in the group of prime order p, therefore does not leak any statistical information about

ADVANTAGE OF PROPOSED SYSTEM:

1) The privilege is possible scheme is defined as similar to the privileges managed in ordinary operating systems
2) Security analysis shows that both AnonyControl and AnonyControl-F are secure under the decisional bilinear Diffie–Hellman assumption

SYSTEM ARCHITECTURE:



INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

MODULE DESCRIPTION:

Number of Modules

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

1. Registration based Social Authentication Module
2. Security Module
3. Attribute-based encryption module.
4. Multi-authority module.

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.

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

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 encryption 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 decrypter's identity has some overlaps with the one specified in the ciphertext.

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

CONCLUSION

This paper proposes a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. Using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information. More importantly, our system can tolerate up to N −2 authority compromise, which is highly preferable especially in Internet-based cloud computing environment. We also conducted detailed security and performance analysis which shows that AnonyControl both secure and efficient for cloud storage system. The AnonyControl-F directly inherits the security of the AnonyControl and thus is equivalently secure as it, but extra communication overhead is incurred during the 1-out-of-n oblivious transfer. One of the promising future works is to introduce the efficient user revocation mechanism on top of our anonymous ABE. Supporting user revocation is an important issue in the real application, and this is a great challenge in the application of ABE schemes.

Making our schemes compatible with existing ABE schemes [39]–[41] who support efficient user revocation is one of our future works.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO. Springer, 1985, pp. 47–53.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT. Springer, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS. ACM, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in S&P. IEEE, 2007, pp. 321–334.

[5] M. Chase, "Multi-authority attribute based encryption," in TCC. Springer, 2007, pp. 515–534.

[6] M. Chase and S. S. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in CCS. ACM, 2009, pp. 121– 130.

[7] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.

[8] V. Bozovi ˇ c, D. Socek, R. Steinwandt, and V. I. Vill ´ anyi, "Multi- ´ authority attribute-based encryption with honest-but-curious central authority," IJCM, vol. 89, no. 3, pp. 268–283, 2012.

[9] F. Li, Y. Rahulamathavan, M. Rajarajan, and R.-W. Phan, "Low complexity multi-authority attribute based encryption scheme for mobile cloud computing," in SOSE. IEEE, 2013, pp. 573–577.

[10] K. Yang, X. Jia, K. Ren, and B. Zhang, "Dac-macs: Effective data access control for multi-authority cloud storage systems," in INFOCOM. IEEE, 2013, pp. 2895–2903.

[11] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT. Springer, 2011, pp. 568–588.

[12] S. Muller, S. Katzenbeisser, and C. Eckert, "On multi-authority ¨ ciphertext-policy attribute-based encryption," Bulletin of the Korean Mathematical Society, vol. 46, no. 4, pp. 803–819, 2009.