ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

An Expressive and Provably Secure Ciphertext-policy Attribute-based Encryption

Ahehtisham Ahamed[1], T.Baba[2]

M.Tech Student, Dept. of CSE, PVKK Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India [1]

Assistant Professor in Dept. of CSE, PVKK Institute of Technology, Affiliated to JNTUA, Andhra Pradesh, India[2]

ABSTRACT: Cloud computing is a revolutionary computing paradigm which enables flexible, on-demand and low-cost usage of computing resources. Those advantages, ironically, are the causes of security and privacy problems, which emerge because the data owned by different users are stored in some cloud servers instead of under their own control. To deal with security problems, various schemes based on the Attribute-Based Encryption have been proposed recently. Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Data security is the key concern in the distributed system. 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 semianonymous 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.

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 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

resilient in the case of security breach in which some part of the system is compromised by attackers.
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, 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 are-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to there-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**.**

II. LITERATURE SURVEY

K. Yang, X. Jia, K. Ren, and B. Zhang[4] This paper describes Data access control is an effective way to ensure the data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems.

W.-G. Tzeng [5], This paper describes propose efficient and secure (string) oblivious transfer (OT1n) schemes for any n

_ 2. We build our OT1 n scheme from fundamental cryptographic techniques directly. The receiver‟s choice is unconditionally secure and the secrecy of the unchosen secrets is based on the hardness of the decisional Diffie-Hellman problem.

S. Yu, C. Wang, K. Ren, and W. Lou[5] This paper describes Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

A. Shamir, [1] This paper introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other 's signatures without exchanging private or public keys, without keeping key directories , and without using the services of a third party. The scheme assumes t h e existence of trusted key generation centers, whose sole purpose is t o give each user a personalized smart card v when he first join st he network.

A. Sahai and B. Waters,[2] This paper introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω_ , if and only if the identities ω and ω are close to each other as measured by the “set overlap” distance metric.

V. Goyal, O. Pandey, A. Sahai, and B. Waters,[3] This paper describes As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

data, is that it can be selectively shared only at a coarse-grained level(i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KPABE).

III. PROPOSED WORK

In this scheme Various schemes based on the attribute-based encryption have been proposed to secure the cloud storage. Various techniques have been proposed to protect the data contents privacy via access control. we propose AnonyControl and AnonyControl-F (Fig. 1) to allow cloud servers to control users‟ access privileges without knowing their identity information.
They will follow our proposed protocol in general, but try to find out as much information as possible individually .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. We firstly implement the real toolkit of a multiauthority based encryption scheme AnonyControl and AnonyControl-F.

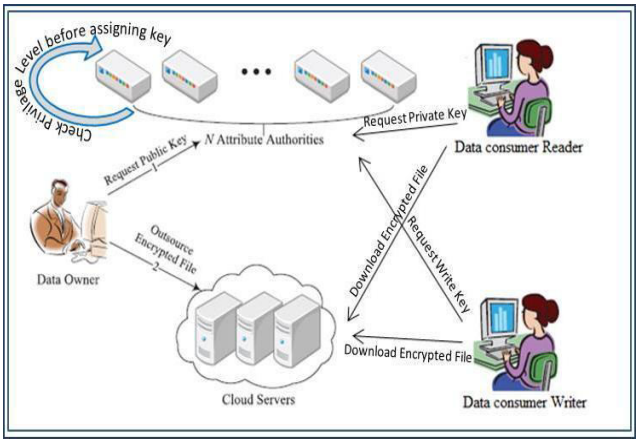

Fig 1.1: architecture of system

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

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 Attribute-based encryption module.
3. 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 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.

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

IV. CONCLUSIONS AND FUTURE WORK

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. We also conducted detailed security and performance analysis which shows that

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 7, July 2019

Anony- Control 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

V. ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be in-complete without mentioning the people who make it possible. I am grateful to number of individuals, faculty members, whose professional guidance along their encouragement have made it very pleasant endeavor to undertake this project. I have a great pleasure in presenting the dissertation **Control Cloud Data Access Using Attribute-Based Encryption** under the guidance of Prof. Sahane Prema B. for giving us the opportunity to work on this topic and their support and also all the teaching and non-teaching staff of Computer Engineering Department for their encouragement, support and untiring cooperation. Finally I express my sincere thanks to our parents, friends and all those who helped us directly or indirectly in many ways in completion of this dissertation work.

REFERENCES

[1] Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
[2] Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 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 *Proc. 13thCCS*, 2006, pp. 89–98.
[4] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.
[5] W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," *IEEE Trans. Comput.*, vol. 53, no. 2, pp. 232–240, Feb. 2004.
[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.