

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

A New Identity Base Encryption for Secure Data Sharing in Cloud Computing

K. Jyothsna Sai¹, V. Narahari², A. Sandhya Rani³

M.Tech Student, Dept of CSE, ALTS Engineering College, JNTUA, AP, India¹

Assistant Professor, Dept. of CSE, ALTS Engineering College, JNTUA, AP, India.²

Assistant Professor & HOD, Dept. of CSE, ALTS Engineering College, JNTUA, AP, India³

ABSTRACT: Cloud computing presents a bendy and convenient way for information sharing, which brings diverse advantages for both the society and individuals. But there exists a herbal resistance for users to immediately outsource the shared facts to the cloud server because the information frequently incorporate precious information. Thus, it's miles essential to area cryptographically more advantageous get entry to control at the shared statistics. Identity-primarily based encryption is a promising cryptographical primitive to build a realistic records sharing gadget. However, access control isn't always static. That is, when some consumer's authorization is expired, there should be a mechanism that can do away with him/her from the system. Consequently, the revoked user cannot get admission to each the formerly and sooner or later shared facts. To this case, we propose a perception referred to as revocable-storage identity-based encryption (RS-IBE), which could provide the forward/backward security of ciphertext through introducing the functionalities of person revocation and ciphertext update simultaneously. Furthermore, we gift a concrete creation of RS-IBE, and prove its security in the defined protection model. The overall performance comparisons indicate that the proposed RS-IBE scheme has blessings in terms of functionality and performance, and as a consequence is feasible for a practical and value-effective information-sharing machine. Finally, we offer implementation effects of the proposed scheme to demonstrate its practicability.

KEYWORDS: 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 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.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals.

• **Data confidentiality:** Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.

• **Backward secrecy:** Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.

• **Forward secrecy:** Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals.

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 (OT_{1n}) schemes for any n

2. We build our OT_{1n} 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 the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the 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 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).

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

III. EXISTING SYSTEM

Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority. Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users.

Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme.

Chen et al. constructed a RIBE scheme from lattices.

DISADVANTAGES OF EXISTING SYSTEM:

The identity is authenticated based on his information for the purpose of access control (or privilege control in this paper).

Preferably, any authority or server alone should not know any client's personal information.

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.

IV. PROPOSED WORK

It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing.

RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period.

A RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.

Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again...

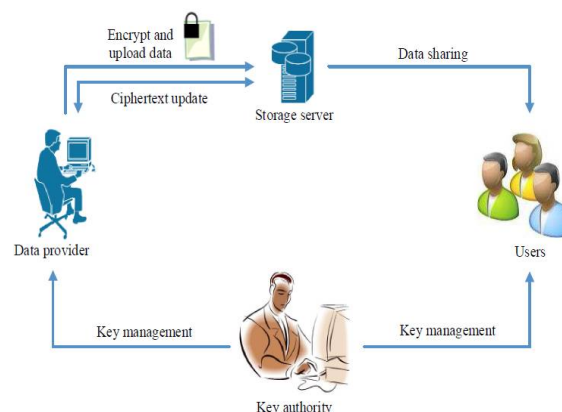


Fig 1.1: architecture of system

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

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 its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

IMPLEMENTATION:

Attribute Authorities:

Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

Data Consumers:

Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

Data Owners:

Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

Cloud Server:

Then, the owner sends the encrypted data to the cloud server together with the cipher-texts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

III. CONCLUSIONS AND FUTURE WORK

In this paper the proposed system achieves fine-grained privilege control and also identity anonymity while conducting privilege control based on users' identity information by using multiple authorities in the cloud computing system. To build a cost-effective and secure data sharing a notion called RS-IBE is proposed, which supports identity revocation and ciphertext update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ -DBHE assumption. The results show that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

REFERENCES

- [1] M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.
- [2] iCloud. (2014) Apple storage service. [Online]. Available: <https://www.icloud.com/>
- [3] Azure. (2014) Azure storage service. [Online]. Available: <http://www.windowsazure.com/>
- [4] Amazon. (2014) Amazon simple storage service (amazon s3). [Online]. Available: <http://aws.amazon.com/s3/>
- [5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

- Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.
- [6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.
- [7] G. Anthes, “Security in the cloud,” *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.
- [8] Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1985, pp. 47–53.
- [9] Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
- [10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Proc. 13th CCS*, 2006, pp. 89–98.
- [11] K. Yang, X. Jia, K. Ren, and B. Zhang, “DAC-MACS: Effective data access control for multi-authority cloud storage systems,” in *Proc. ICSE INFOCOM*, Apr. 2013, pp. 2895–2903.
- [12] W.-G. Tzeng, “Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters,” *ICSE Trans. Comput.*, vol. 53, no. 2, pp. 232–240, Feb. 2004.
- [13] 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,” *ICSE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.