International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

Identity-Based Encryption with Outsourced Revocation in Cloud Computing

SIVARANJANI.J, M.Phil (Computer Science)
RAJAH SERFOJI GOVERNMENT COLLEGE (Autonomous),
Thanjavur - 613 005
jsivani13@gmail.com

Mr. C.MURUGANANDAM, M.Sc., M.phil.,
Assistant professor in Department of Computer Science
RAJAH SERFOJI GOVERNMENT COLLEGE (Autonomous),
Thanjavur - 613 005

Abstract — Cloud computing provides a simplest way of data sharing, it provides various benefits to the users. But directly outsourcing the shared data to the cloud server will bring security issues as the data may contain valuable information. Hence, it is necessary to place cryptographically enhanced access control on the shared data, named Identity-based encryption to build a practical data sharing system. when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. Thus, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which introducing the functionalities of user revocation and cipher text update simultaneously.

Keywords: Revocation, Encryption, Key Exchange, Private key generator, cipher text.

1. INTRODUCTION

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of computing resources (eg. Networks, servers, storage and services).In the earliest stage of cloud computing security is provided by Certificate Based Encryption which encrypt the data based on certificate which is provided to the data user. Unauthorized user may duplicate the certificate which may lead to security issue. To overcome the issue, Identity Based Encryption replaces this technique. In which the user's id (name, email address, ip address, port number, etc.) is used to generate the keys which are used to encrypt the data. This does not provide security to data shared in cloud because the data is stored for a longer period by then the data is accessible to the third party very easily. To avoid this Identity Based Encryption With Efficient Revocation was introduced. In this approach the data provider can provide the life time of the key provided

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

to the user. At the end of the life time the user can revoke the key with the help of central authority called Private Key Generator (PKG). After this Revocable Storage Identity Based Encryption is proposed, this provides both forward and backward security which is absent in previous technique. This technique allows the data provider to specify the life time of the data shared as well as the private key provided to the data user. Once this time expires the private key generator (pkg) is responsible for revoking the cipher text and private key of each user. This mechanism of providing security in both the ends is called as forward and backward security.

2. LITERATURE SURVEY

L. 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.

In this paper we investigate the concept of Cloud Computing to achieve a complete definition of what a Cloud is, using the main characteristics typically associated with this paradigm in the literature. More than 20 definitions have been studied allowing for the extraction of a consensus definition as well as a minimum definition containing the essential characteristics. This paper pays much attention to the Grid paradigm, as it is often confused with Cloud technologies. We also describe the relationships and distinctions between the Grid and Cloud approaches. Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a payper-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs. On the other hand, looking for the minimum common denominator would lead us to no definition as no single feature is proposed by all definitions. The set of features that most closely resemble this minimum definition would be scalability, pay-per-use utility model and virtualization.

Finally, QoS and SLA enforcement will also be essential before ICT companies reach high levels of confidence in the Cloud. Usability and virtualization could also be applied to grids to ease their usage, enhance their scalability, and allow on-demand services. NGG and OGF efforts are highly devoted to this task, enforcing standardization to enable a Cloud federation that can then deal with the required massive scalability.

B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.

With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Some existing remote integrity checking methods can only serve for static archive data and, thus, cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. In this paper, we first design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.

.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

3.PROBLEM STATEMENT:

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographically tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data.

4. EXISTING SYSTEM

- The concept of identity-based encryption was introduced by Shamir and conveniently instantiated by Boneh and Franklin. IBE eliminates the need for providing a public key infrastructure (PKI).

- In the traditional PKI setting, the problem of revocation has been well studied and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE.

To conquer this problem, 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.

Proposed System

A dynamic access control system via Revocable Storage Identity Based Encryption (RS-IBE) is proposed that facilitates forward/backward security of data through efficient revocation mechanism of user and updates policy of ciphertext. It prevents access of data by revoked user.

- The procedure of ciphertext update only needs public information. Note that no previous identity-based encryption schemes in the literaturecan provide this feature;

- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time periods. More precisely, the following achievements are captured in this paper:

- We provide formal definitions for RS-IBE and its corresponding security model;

- We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously;

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure.

Advantages of Proposed System

We provide formal definitions for RS-IBE and its corresponding security model; 2. We present a concrete construction of RS-IBE. 3. The proposed scheme can provide confidentialityand backward/forward secrecy simultaneously. 4. We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear DiffieHellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure. 5. The procedure of cipher text update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature; 6. The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time period.

5. IMPLEMENTATION

In this proposed system we represent a model for the outsourced revocable IBE by using the system architecture which has been compared with IBE scheme.

The proposed methodology describes, secure data sharing system can provide confidentiality and backward secrecy. In this paper, we introduce a notion called revocablestorage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

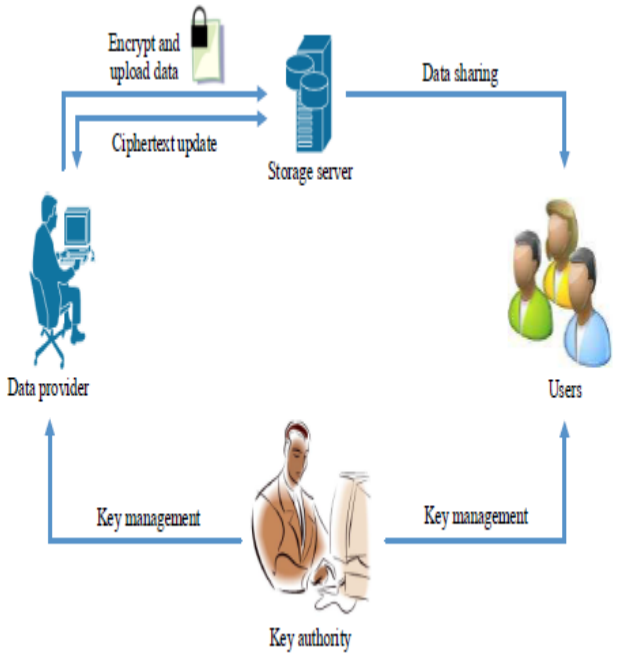
- We provide formal definitions for RS-IBE and its corresponding security model;
- We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward secrecy simultaneously;
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure;

The proposed scheme is efficient in the following ways:

- The procedure of ciphertext update only needs *public information*. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time periods.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

7. SYSTEM MODEL



8. CONCLUSION AND FUTURE WORK

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, 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. Furthermore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

9. REFERENCES:

[1] Alexandra Boldyreva (Georgia institute of technology, Atlanta, GA, USA), Vipul Goyal (university of California at Los Angeles, CA, USA) and Virendra Kumar (Georgia institute of technology, Atlanta, GA, USA) "Identity-based encryption with efficient revocation" 2008.

[2] Chul Sur Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea, Youngho Park (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea), Sang UK Shin (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) Kyung Hyune Rhee (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) "Certificate-Based Proxy Reencryption for Public Cloud Storage 2013".

[3] Mohan, Prakash, and Ravichandran Thangavel. "Resource Selection in Grid Environment Based on Trust Evaluation using Feedback and Performance." American Journal of Applied Sciences 10.8 (2013): 924.

[4] Prakash, M., and T. Ravichandran. "An Efficient Resource Selection and Binding Model for Job Scheduling in Grid." European Journal of Scientific Research 81.4 (2012): 450-458.

[5] Jin Li (School of Computer Science, Guangzhou University, Guangzhou, China),Wenjing Lou (Virginia Polytechnic Institute and State University, Blacksburg) "Identity based encryption with outsourced revocation in cloud computing" 2015.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 2, No 01, 2017 ISSN: 2348-6600
Reference ID: IJCS-304 PAGE NO: 2035-2041

[6] Prakash, M., R. Farah Sayeed, S. Princey, and S. Priyanka. "Deployment of MultiCloud Environment with Avoidance of DDOS Attack and Secured Data Privacy." International Journal of Applied Engineering Research 10, no. 9 (2015): 8121-8124.

[7] Annamalai, R., J. Srikanth, and M. Prakash. "Integrity and Privacy Sustenance of Shared Large Scale Images in the Cloud by Ring Signature." International Journal of Computer Applications 114.12 (2015).