ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

REVOCATION FUNCTIONALITY AND EFFICIENT KEY GENERATION USING IDENTITY BASED ENCRYPTION

Ms. [1]K.Rupiya, Mr.[2]K.Anbuselvan, M.E, Mr.[3]S.Aravindh, M.Tech., M.B.A.,

[1]Pursuing M.Tech, CSE Branch, Dept of CSE, [2]Assistant Professor, Department of computer science and Engineering, [3]Assistant Professor, Department of Computer science and Engineering, Gojan School of Business and Technology, Edapalayam, Redhills, Chennai.

Abstract: . This paper presents an numerous services in cloud computing, the cloud can give a more adaptable and easy way to share the data which provides various benefits to our environment. However it also suffers from several security issues and privilege problems between user and subsequently shared data. As a result, the outsourcing data to cloud user want to control access to this data at the same time authorized users only can share the data. The proposed approach named as revocable identity based encryption can meet the security goals as data discretion and privacy problems. RIBE features a mechanism that enables a sender to append the current time period to the cipher text so that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period. Such a data sharing system can provide discretion and backward secrecy. In addition, the method of decrypting and re-encrypting all the shared data can make certain forward secrecy. This proposal has advantage requisites of functionality and competence, and thus is possible for a realistic and producing good result with effective cost benefits .

***Keywords*:** cloud computing, encrypting, decrypting, cipher text, security issues

INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Encrypting the data before storing in cloud can handle the confidentiality issue.

Furthermore, to overcome the security threats, such kind of identity based access control placed on the shared data should meet the following security goals[1].

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[1].

Backward secrecy: It means that, when a user's authorization is expired, or user's secret key compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity[1].

Forward secrecy: It means that, when a user's authorization is expired, or user's secret key compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her[1].

Identity-based (ID-based) cryptosystem, initiated by Shamir, eradicated the need for confirming the authority of public key certificates, the administration of which is both time and cost consuming. In this cryptosystem, the public key of each user is easily assessable from a string corresponding to the user publicly Known identity (e.g., an email address, a housing address, etc.). A private key generator (PKG) then calculates private keys from its master secret for users. This

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

functionality keeps away from the need of certificates (which are essential in traditional public-key structure) and connects an implicit public key (user identity) to each user within the system[5].
Outsourcing data to cloud server implies that data is out control of user. This may cause user's hesitation since the outsourced data usually contain valuable and sensitive information[1].

Since shared data is outsourced to the cloud and users no longer store it on local devices, the straightforward method to re-compute these signatures during user revocation is to allow an existing user to first download the blocks signed by the revoked user, verify the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. However, this straightforward method may cost the existing user a huge amount of communication and computation resources by downloading and verifying blocks, and by re-computing and upload signatures, especially when the number of re-signed blocks is quite large or the membership of the group is frequently changing. To make matters worse, the size of shared data in the cloud is generally large, which further prevents existing users from downloading and re-signing data efficiently. Clearly, if the cloud could possess each user's private key, it can easily finish the re-signing task for existing users without asking them to download and re-sign blocks. However, since the cloud is not in the same trusted domain with each user in the group, outsourcing every user's private key to the cloud would introduce significant security issues[4].

The rest of this paper is organized as follows. In Section 2 related works are introduced. Section 3 deals with the proposed work which describes the relevance feedback approach, finally section 4 concludes the paper.

2.RELATED WORK

Jianghong Wei, Wenfen Liu, Xuexian Hu[1] Introduced a notion called revocable storage identity-based encryption(RS-IBE) for building a cost effective data sharing system that fulfils the security goals. Identity based encryption is a promising cryptographically primitive to build a practical data sharing system. However access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system consequently, revoked user cannot access both the previously and subsequently shared data. This paper present a concrete construction of RS-IBE, and prove its security in the defined security model.

C. Wang, S. S. Chow, et al [2] To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, propose a secure cloud storage system supporting privacy-preserving public auditing. Further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

B. Wang, B. Li, and H. Li [3] proposed a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing proxy re-signatures, this paper 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. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

K. Yang and X. Jia [4] In this paper, propose an efficient and secure protocol to address these issues. The method allows third party auditor to periodically verify the data integrity stored at CSP without retrieving original data. The challenge-response protocol transmits a small, constant amount of data, which minimizes network communication. Most importantly, protocol is confidential: it never reveals the data contents to the malicious parties. The proposed scheme also considers the dynamic data operations at block level while maintaining the same security assurance. A solution removes the burden of verification from the user, alleviates both the user's and storage service's fear about data leakage and data corruptions.

K. Chard, K. Bubendorfer, et al [5] Introduced a business application as a means of regulating sharing, due to the unique nature of the Social Cloud. The

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

business application is innovative as it uses both social and economic protocols. In today's world, social community credentials are being used for authentication purpose on various other websites (e.g. Face book). Here, this paper outline our vision of creating a Social Storage Cloud, looking especially at possible market mechanisms that could be used to create a dynamic Cloud infrastructure in a Social network environment.

X. Huang, J. Liu, S. et al [6] In this paper, additionally improve the safety of ID-based ring signature by giving advance security: If a secret key of any user has been compromise, all earlier produced signatures that contain this user still remains legal. This property is particularly significant to any huge scale data distribution system, since it is unfeasible to request all data owners to re-authenticate their data still if a secret key of one single user has been compromised. This paper offer an actual and well-organized instantiation of our scheme, demonstrate its safety and supply an accomplishment to illustrate its realism.

3. PROPOSED WORK

The relevance feedback techniques contains the following strategies.

3.1 Data upload and user data request.

First we need to done the registration process for user, data provider and admin. While doing registration they want to select their role. If the registrations success they can login with their mail id and password. In worst case the system will throw messages as invalid login. After login the data provider will upload the data, then user send request to data provider.

3.2 Data provider key request and Key generation

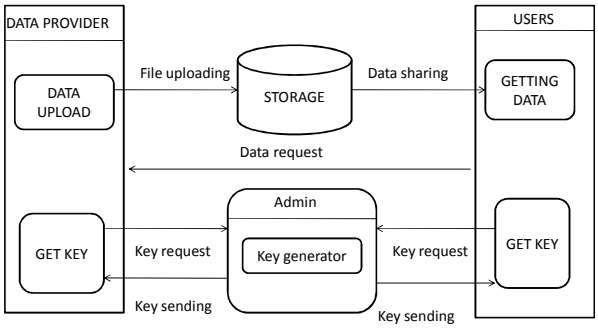
User will give the request to the data provider for accessing the shared data in cloud server. When the request getting from the user, after data provider will alert the key generator to produce the user id based key. Then the key generator will send key to both data provider and user.

3.3 Identity Based encryption the data

Data provider getting key from key generator, using that key data provider will encrypt data and stored into database. Whenever getting the new request from the user that time re-encrypts the data using new key, also uploading in database.

3.4 User getting data based on time

User getting the decryption key from key generator. Key generator Mention the time period for key valid, after that time period user authorization will expired also user cannot access the previously added data and



subsequently data from the cloud server.

3.5 ARCHITECTURE

Data provider first decides the user (e.g., Shamir and david) who can share the data. Then Shamir encrypt the data under the identities Shamir and david, and upload the ciphertext of the shared data to the cloud server. When either Shamir or david 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. In some cases , e.g Shamir's authorization get expired, George can download the ciphertext of the shared data, and then decrypt-the-re-encrypt the shared data such that Shamir is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

Users give data request to data provider for file, then data provider give alert message to key generator afterwards, Admin or key generator to generate the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Special Issue 6, March 2017

secret key for both data provider and user. Admin can send the key to user and data provider. Finally data provider can upload the file into cloud storage.

CONCLUSION

Cloud computing brings great expediency for people. Predominantly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to building a cost-effective and secure data sharing system in cloud computing, proposed a perception called RS-IBE, which supports identity revocation and ciphertext update at the same time such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. In the addition, a actual building of RS-IBE is created. This proposal has advantage requisites of functionality and competence, and thus is possible for a realistic and producing good result with effective cost benefit.

REFERENCE

[1] Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," *Journal Of Latex Class Files, Vol. 14, No. 8, August2015*

[2] 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.

[3] 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.

[4] 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.

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563,2012.

[6] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, 2014, doi:10.1109/TC.2014.2315619.

[7] G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.

[8] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 384–394 2014.

[9] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng,"Key-aggregate cryptosystem for scalable data sharing in cloud storage," *Parallel and Distributed Systems, IEEE Transactions on*,

[10] A. Shamir, "Identity-based cryptosystems and signature schemes,"in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[11] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[12] S. Micali, "Efficient certificate revocation," Tech. Rep., 199