International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure Data Sharing in Cloud Computing Using Revocable Storage Identity-based Encryption Methodology: A Survey

Ms. Vinaya Reddy S
School of computer Science and IT, Jain University (Deemed-to-be University), Bangalore Karnataka, India

Dr. J. Bhuvana
School of computer Science and IT, Jain University (Deemed-to-be University), Bangalore Karnataka, India

ABSTRACT- Cloud computing is one of the best ways to store, retrieve and share data which is easy, convenient and also beneficial for both the organization and individuals. But there are many of disadvantages because of which users hesitate to share data to the cloud as they contain important and valuable information. Therefore it is necessary to apply encryption on your user's shared data, for this Identity-based encryption is one of common and promising approach to secure shared data. 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, the revoked user cannot access both the previously and subsequently shared data.

To overcome this problem Revocable-storage identity-based encryption (RS-IBE) is introduced, which can provide the forward/backward security of cipher text with functionalities like user revocation and cipher text update that takes place simultaneously. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data sharing system.

Keywords - Cloud computing, data sharing, revocation, Identity-based encryption, cipher text update, decryption key

1. INTRODUCTION

CLOUD computing is a platforms provides huge computing capacity and memory space at a low cost. It helps users to get expected services irrespective of time and location across multiple platforms such as mobile devices, personal computers, etc. and thus brings great convenience to the users. Among various services provided by cloud computing, cloud storage service, such as Drop box, Microsoft's Azure, and Amazon's S3, etc. can provide easy and flexible way to share data over

the Internet, which provides various benefits for Cloud users.

However, it also has to face a lot of security threats, which are the primary concerns of cloud users. First and foremost, outsourcing data to a cloud server means that data is out of the control of users. This is why users hesitate because the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and maleficent environment, and cloud servers can become a target of any malicious attacks. Even worse, the cloud server itself may reveal users' data for illegal profit. Lastly, data sharing is dynamic. That is, when a user's authorization gets expired, he or she should no longer have the right to access the old and subsequently shared data. Therefore, while outsourcing data to cloud servers, users also want to control access to these data such that only current authorized users can share the outsourced file or data. One of the solution to overcome this problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Additionally to overcome the above security threats, identity-based access control placed on the shared data should fulfill the following security goals:

Data Secrecy: Unauthorized users must be prevented from accessing the plaintext of the shared data stored in the cloud. In addition, the cloud server should also be discouraged from knowing the plaintext of shared data.

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

Forward secrecy: When a user's authority is expired, or when a user's secret key is compromised, he or she must be prevented from accessing the plaintext of the shared data that was previously accessed by him or her. The important and main problem addressed in this paper is how to build a fundamental identity-based crypto-graphical tool to achieve full security. We also found that there are other security issues that are equally important for a realistic system of data sharing, such as the availability and authenticity of the shared data

2. LITERATURE REVIEW

1) Towards Cloud definition- A break in cloud

AUTHORS: L. M.Vaquero, L.Rodero-Merino, J.Caceres and M. Lindner

This paper discusses the conception of Cloud Computing to get full description of what a Cloud is, using the important characteristics generally related to this paradigm within the literature. About 20 definitions are studied with the extraction of a consensus definition yet as a minimum definition containing the essential characteristics. This paper pays more attention to the Grid paradigm, because it is usually confused with Cloud technologies. It also explains the relationships and distinctions between the Grid and Cloud approaches.

2) A vision for socially motivated resource sharing - Social Cloud Computing

AUTHORS: K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana

Online connections in social networks frequently supports real world connections or relationships, thus used to infer league of trust between users. This model leverages these connections to make a dynamic "Social Cloud," thereby enabling users to share heterogeneous resources within the environment of a social network. Additionally, the essential social corrective mechanisms (incentives, disincentives) is oriented to enable a cloud-based framework for long run sharing with lower privacy concerns and security overheads than are present in traditional cloud environments. Because of the distinctive complexion of the Social Cloud, a social market place is suggested as a way of regulating sharing. The social market is novel, because it uses both social and profitable protocols to facilitate trading. This paper defines Social Cloud computing, outlining various aspects of Social Clouds, and demonstrates the approach employing a social storage cloud implementation in Facebook.

3) Privacy preserving public auditing for secure cloud storage

AUTHORS: C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou,

Using cloud storage, users can casually store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the load of local data storage and maintenance. But the fact that users don't have physical ownership of the assigned data makes the information integrity protection in cloud computing an alarming task, mainly for users with restriction computing resources. However, users should be able to only use the cloud storage as if it is local, without concern about the necessity to verify its honesty. Consequently, authorizing public survey for cloud storage is of crucial significance so that users can resort to a third-party auditor (TPA) to find the honesty of outsourced data and be worry free. To safely launch a good TPA, the auditing process should not have new vulnerabilities toward user data privacy and establish no additional online load to user. A secure cloud storage system supporting privacy-preserving public auditing is proposed in this paper. Additionally results extend to enable the TPA to perform checkups for multiple users at the same time and efficiently. Expensive security and performance analysis show the proposed schemes are provably secure and largely effective. Primary

experiment performed on Amazon EC2 instance demonstrates the fast performance of the design.

4) Secure and efficient dynamic auditing protocol for data storage in cloud computing

AUTHORS: K. Yang and X. Jia

In cloud computing, data providers or owners host or upload their data on cloud servers and users access the data or information from cloud servers. On account of information or data outsourcing, this new paradigm of information or data hosting service introduces new security challenges, which needs an independent auditing service to test the data honesty within the cloud. Some existing remote integrity checking methods can only be used for static archive data hence, can't be applied to the auditing service as the info within the cloud can be dynamically updated. Like this efficient and secure dynamic auditing protocol is apt to assure data owners that the data is correctly stored within the cloud. In this paper, first design of auditing framework for cloud storage systems is introduced and efficient and privacy-preserving auditing protocol is proposed. Next, auditing protocol is continued to support the info or data dynamic operations, which is capable and provably secure within the random oracle model. And also to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that the proposed auditing protocols are immune and adequate, especially to reduce the computing cost of the auditor.

5) Public auditing for shared data using efficient user revocation

AUTHORS: B. Wang, B. Li, and H. Li

With data storage and sharing services within the cloud, users can easily modify and share data in groups. To make sure shared data honesty can be verified publicly, users in the group need to cipher signatures on all the blocks in shared data. Different blocks in shared data are commonly signed by different users since data modifications are performed by different users. Considering security needs, a revoked user from the group and the blocks which were already signed by the revoked user should be re-signed by current user. This method, which allows an existing user to download the identical- part of shared data and re-sign in during user revocation, is faulty due to massive size of shared data. In this paper, a completely unique public auditing mechanism for the honesty of shared data is proposed with impressive user revocation. By adopting the idea of proxy re-signatures, we allow the cloud to re-sign blocks on account of existing users during user revocation, so the existing users need not download and re-sign blocks on their own. Additionally, a public verifier checks the honesty of shared data without restoring the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Besides, this structure supports batch auditing by verifying multiple auditing functions concurrently. Experimental results show that this mechanism can significantly improve the productivity of user revocation.

3. Discussion and Methods

It seems that the concept of revocable identity-based encryption (RIBE) is a promising approach for the security requirements of data sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher-text such that the receiver can decrypt the cipher-text only under the condition that he/she is not revoked at that time period. RIBE-based data sharing system works as follows:

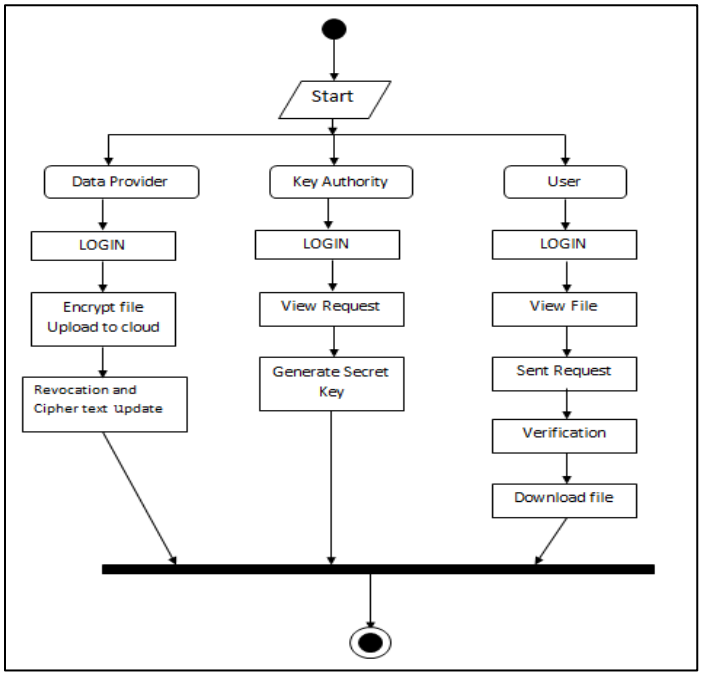

Fig.1.1

Step 1: The data provider (e.g., Varun) first decides the users (e.g., Alisha and Ram) who can share the data. Then, Varun encrypts the data under the identities Alisha and Ram, and uploads the cipher-text of the shared data to the cloud server.

Step 2: When either Alisha or Ram wants to get the shared data, she or he can download and decrypt the corresponding cipher-text. 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., Alisha's authorization gets expired, Varun can download the cipher-text of the shared data, and then decrypt-then-re-encrypt the shared data such that Alisha is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

4. Conclusion

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper we explored the problems of encryption and Identity-based encryption to overcome and build a cost-effective and secure data sharing system in cloud computing, RS-IBE is introduced, which supports identity revocation and cipher-text 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 use.

Reference

[1] 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.

[2] 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] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

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

[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] 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.

[6] 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.

[7] 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.

[8] 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, vol. 25, no. 2, pp. 468–477, 2014.

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

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

[11] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[12] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[13] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.

[14] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.

[15] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial

Cryptography and Data Security. Springer, 2007, pp. 247–259.

[16] A Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.

[17] B Libert and D. Vergnaud, "Adaptive-id secure revocable identitybased encryption," in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15.

[18] "Towards black-box accountable authority IBE with short cipher-texts and private keys," in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.

[19] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in Information Security and Privacy. Springer, 2012, pp. 390–403.