ISSN (online) : 2277-5390
ISSN (Print): 2277-5382

A survey on data security mechanism for cloud storage system

M. Vimala[1], K.Vishnukumar[2]

[1]*P.G. Scholar,* [2]*Head, Dept. of Computer Science, KPR Institute of Engineering and Technology, Coimbatore-6411407, TN, India*
[1]vimalamphil2016@gmail.com, [2]vishnukumarkpr2016@gmail.com

Abstract

Objectives: To analysis various mechanisms to improve the security of cloud storage system.
Methods: The methods such as unidirectional proxy re-encryption schemes, Identity-Based Proxy Re-Encryption system, third party auditor scheme, NCCloud, certificate based signature scheme and two-factor data security protection mechanism are analyzed in this paper.
Findings: In this paper various cloud storage data security protection techniques are compared through their merits and demerits of the technique to prove two-factor data security protection is better than other techniques. Encryption is the most effective technique to transmit the sensitive data in cloud environment. The findings of this work prove that the two-factor data security protection mechanism provides better result than other approaches.

Keywords: cloud storage system, cloud security, cloud protection, two-factor data security protection.

1. Introduction

Cloud computing has been visualized as the next generation of distributed computing in an emerging network field. The National Institute of Standards and Technology (NIST) describes emerging cloud environment by four deployment models [1], five essential characteristics [2] and three service models. The three models are infrastructure as a service (IAAS) [3], platform as a service (PAAS) [4], and software as a service (SAAS) [5]. The characteristics of cloud computing are broad network access, location-independent resource pooling, rapid resource elasticity, on-demand self-service and measured service. The three service models in cloud are private cloud, public cloud, community cloud, and hybrid cloud.

The data stored in cloud environment can be accessed from anywhere and at anytime and by anyone. Many techniques effectively provide the security for cloud storage data. During transmission of data in cloud environment, encryption is an efficient and widely used technique for data security. It can be done by public key, private and other identical information between the sender and receiver.

In [6] proposed an architecture that ensures the privacy of data stored in cloud storage. The proposed architecture can directly applicable to existing clouds without any modifications or any changes in cloud database. It can be process that connects directly to an encrypted cloud database without an intermediate devices or systems with geographically distributed clients and it also allowed executing independent and operations including those changing the database structure. Moreover the proposed architecture removes intermediate proxies that limit the scalability, elasticity and availability properties that are intrinsic in cloud-based solutions.

In [7] described unidirectional proxy re-encryption schemes. This scheme is with chosen cipher text security in the standard model. The two contribution of this proposed system is fitted a unidirectional extension of the Canetti–Hohenberger security model and another one is how to change the scheme to attain security. It provides additional properties like as non-interactive temporary delegations.

In [8] proposed a solution for problem of efficiently delegating in key revocation [9] and generation in Identity Based Encryption (IBE) scheme. In this paper proposed realization of RHIBE, it is constructed based on the scheme called Boneh-Boyen HIBE (BB-HIBE) scheme. The size of ciphertext and revocation cost was same for both RHIBE and BB-HIBE schemes. But in RHIBE allows hierarchical structure of entities and selective ID was protected under Decisional Bilinear Diffie-Hellman (DBDH) assumption.

In [10] proposed new definition and security models for single-hop Identity-Based Proxy Re-Encryption (IBPRE) systems. This system holds the property of IBPRE along with conditional re-encryption technique. This new IBPRE overcome two problems are extension of IBPRE to support conditional re-encryption and construction of CCA-secure unidirectional singlehop IBPRE without random oracles.

In [11] presented a security definition against chosen ciphertext attack (CCA). This definition was for the purpose of certificateless proxy re-encryption. The proposed security model was allowed to adaptively corrupt users. After the corruption of security model and it displayed some proofs to show that a challenges involved in the construction of secure CL-PRE. Finally proved RCCA was secured in random oracle model.

In [12] proposed a solution for constructing a multi-use unidirectional IBPRE scheme problem by converting non-anonymous hierarchical identity-based encryption (NaHIBE) with strongly CPA security to CCA-secure and collusion-resistant multi-use unidirectional IDbased proxy re-encryption MUIBPRE. This technique tries to satisfy the security requirements are CCA security and collusion resistance.

In [13] proposed an approach to protect user's privacy data in cloud environment. This approach explained the compression applied in secret keys in public key cryptosystem to handle the cloud storage by supporting delegation of secret keys in various cipher text classes. This approach is more flexible and efficient than hierarchical key assignments. The hierarchical key assignments analyzed privileges of all key-holders if they allocate the same privileges it saved their space for privileges. The proposed approach used key-aggregate cryptosystem encryption technique where the cipher texts were categorized into various classes.

In [14] proposed an effective third party auditor (TPA) for privacy preserving public auditing to secure a cloud storage system. This technique allows without learning the data content in a cloud environment an external auditor audit user's outsourced data by using privacy-preserving auditing protocol. This technique used random masking and homomorphic linear authenticator as privacy-preserving auditing protocol. Thus this technique removed burden for cloud user's and expensive task in cloud.

In [15] presented a proxy-based storage system called NCCloud for fault-tolerant multiple-cloud storage. This system was developed on functional minimum-storage regenerating a network a network-coding-based storage scheme. This proposed system used less repair traffic than redundancy as in traditional erasure codes that sustain less monetary cost due to data transfer. This system removes the encoding operations within the storage nodes during repair thus it reduced the repair traffic in the cloud.

In [16] proposed a short and efficient certificate based signature (CBS) scheme to improve level of trust in cloud environment. This scheme was need one group element for public key and the signature size and it reduced the public information to one group elements for each and every user in the cloud environment. This key size is smaller than the PKI based signature scheme because it needs one group element for generation of public key and the another group element is needed for the certificate.

In [17] proposed an approach that overcomes the problem in Attribute-Based Encryption (ABE). In this introduced a cipher text delegation procedure that re-encrypted a cipher text based on the public information and analyzed the problem of revocable in existing Attribute-Based Encryption technique. Based on the analysis it is necessary for first fully secure construction, it modifies an existing Attribute-Based Encryption scheme. Thus this approach was used for revocation on stored data.

In [18] proposed a two-factor data security protection mechanism for cloud storage system. In this proposed mechanism sender sends their data to receiver with an encrypted message. The receiver decrypts the message with the help of secret key of the computer and unique personal security device. If the device is stolen by someone it can be revoked by implementing some algorithms to change the ciphertext. This technique is more transparent to the sender. Moreover this technique decrypts any ciphertext at any time.

Comparison of cloud data security techniques

Ref no	Title	Merits	Demerits
[6]	Distributed, concurrent, and independent access to encrypted cloud databases	Eliminates intermediate proxies and doesn't need modifications in the database structure	Encrypted database results negligible overhead
[7]	Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption	Mild complexity assumptions in bilinear groups	The problem of securely obfuscating CCA-secure re-encryption
[8]	Efficient Delegation of Key Generation and Revocation Functionalities in Identity-Based Encryption	It reduced excessive workload	It has more complicating key distributing method
[10]	A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles	It provides security against adaptive identity and adaptive condition chosen-ciphertext attacks	CHK transformation to achieve CCA Security seems un widely
[11]	Towards a Secure Certificateless Proxy Re-Encryption Scheme	computation time for an exponentiation and a bilinear pairing is lesser than IB-PRE scheme	Results are based on honest list created by challenger
[12]	Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption	CCA security is high	Cipher text size and decryption time will be increased with the number of translations.
[13]	Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	This approach do not need to set a very high number of classes to have better compression	The cipher text size is dependent on the maximum number of ciphertext classes
[14]	Privacy-Preserving Public Auditing for Secure Cloud Storage	Removes cloud user's burden and expensive task	privacy-preserving public auditing protocol is not used in multi-user setting
[15]	NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds	Reduced the repair traffic	It leads to bad repair if don't check the rMDS property
[16]	Short and Efficient Certificate-Based Signature	The computation requirement of CBS is very light	It requires both the public key and user identity for encryption.
[17]	Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption	It satisfies strong efficiency guarantees with consideration of the lifetime of the database.	It creates inconvenience once the current period key is lost
[18]	Two-Factor Data Security Protection Mechanism for Cloud Storage System	Provides confidentiality of data and revocability of the device	It affects from the largest price in Updated Ciphertext Size

2. Conclusion

Various techniques are available to provide security for cloud storage data. Among them, two-Factor Data Security Protection mechanism only provides confidentiality of the data and revocability for cloud data by using secret key and unique personal device.

3. References

1. H. Ziglari, S. Yahya. Deployment models: Enhancing security in cloud computing environment. In: *2016 22nd Asia-Pacific Conference on Communications (APCC)*, IEEE. 2016; 204-209.
2. F. F. Moghaddam, M. B. Rohani, M. Ahmadi, T. Khodadadi, K. Madadipouya. Cloud computing: Vision, architecture and Characteristics. In: *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)*, IEEE. 2015; 1-6.
3. X. Wu, M. C. Wang, W. Zhang, Y. Guo. Cloud program with a pricing strategy for IaaS in cloud computing. In *Parallel and Distributed Processing Symposium Workshops & Ph.D. Forum (IPDPSW), 2012 IEEE 26th International,* IEEE. 2012; 2316-2319.

4. Y. Jinzhou, H. Jin, Z. Kai, W. Zhijun. Discussion on private cloud PaaS construction of large scale enterprise. In: *2016 IEEE International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, IEEE. 2016; pp. 273-278.
5. X. Cao, L. Xu, Y. Zhang, W. Wu. Identity-based proxy signature for cloud service in saas. In: *2012 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS)*. IEEE. 2012; 594-599.
6. L. Ferretti, M. Colajanni, M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. *IEEE transactions on parallel and distributed systems*, 2014; 25(2), 437-446.
7. B. Libert, D. Vergnaud. Unidirectional chosen-ciphertext secure proxy re-encryption. IEEE Transactions on Information Theory. 2011; 57(3), 1786-1802.
8. J. H. Seo, K. Emura. Efficient delegation of key generation and revocation functionalities in identity-based encryption. In: *Cryptographers' Track at the RSA Conference*. Springer Berlin Heidelberg. 2013; 343-358.
9. R. R. Pavithra, V. R. Nagarajan. A survey on certificate revocation scheme using various approaches. *Indian Journal of Innovations and Developments*. 2016; 5(5), 1-3.
10. K. Liang, Z. Liu, X. Tan, D. S. Wong, C. Tang. A CCA-secure identity-based conditional proxy re-encryption without random oracles. In: *International Conference on Information Security and Cryptology*. Springer Berlin Heidelberg. 2012; 231-246.
11. H. Guo, Z. Zhang, J. Zhang, C. Chen. Towards a secure certificateless proxy re-encryption scheme. In: *International Conference on Provable Security*. Springer Berlin Heidelberg. 2013; 8209, 330-346.
12. J. Shao, Z. Cao. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. *Information Sciences*, 2012; 206, 83-95.
13. C.K. Chu, S.S. Chow, W.G. Tzeng, J. Zhou, R.H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. *IEEE Transactions on Parallel and Distributed Systems*. 2014; 25(2), 468-477.
14. C. Wang, S.S. Chow, Q. Wang, K. Ren, W. Lou. Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on computers*. 2013; 62(2), 362-375.
15. H.C. Chen, Y. Hu, P.P. Lee, Y. Tang. NCCloud: a network-coding-based storage system in a cloud-of-clouds. *IEEE Transactions on Computers*, 2014; 63(1), 31-44.
16. J.K. Liu, F. Bao, J. Zhou. Short and efficient certificate-based signature. In: *International Conference on Research in Networking*. Springer Berlin Heidelberg. 2011; 167-178.
17. A. Sahai, H. Seyalioglu, B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In: *Advances in Cryptology–CRYPTO 2012*. Springer Berlin Heidelberg. 2012; 199-217.
18. J.K. Liu, K. Liang, W. Susilo, J. Liu, Y. Xiang. Two-Factor Data Security Protection Mechanism for Cloud Storage System. *IEEE Transactions on Computers*, 2016; 65(6), 1992-2004.

The Publication fee is defrayed by Indian Society for Education and Environment (iSee). www.iseeadyar.org

Citation:

M. Vimala, K. Vishnukumar. A survey on data security mechanism for cloud storage system. *Indian Journal of Innovations and Developments.* 2016; 5 (9), September.