International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 11: November 2015, pp 29-31. www.aetsjournal.com ISSN (Online) : 2394-6237

A Survey on Actor based data retrieval using attribute based encryption in cloud

Priyadharshini P, Revathi M

Abstract— In this paper, we discuss about the cloud computing techniques which enables flexible, on-demand, and low-cost usage of computing resources, but the data is outsourced to some cloud servers, and various privacy concerns emerge from it. In particular, we discuss various schemes that have been proposed to keep the cloud storage secure using attribute-based encryption. We propose dual system encryption methodology for making our cloud storage is more secure. Related papers are analyzed and its advantages and disadvantages are discussed.

Keywords— Anonymity, 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'. Cloud computing is emerging paradigm provides various IT related services. Various techniques have been proposed to protect the data contents privacy via access control. The attribute based encryption which will execute through quantum cryptography, which deals with both mining and architectural design. (i.e) both data mining and networking can be implemented here. This method will be named as data engineering methodology. Anonymous, in a general computing context, means keeping a user's name and identity concealed through various applications. For security, an application may require that user's names be kept anonymous in order to maintain their privacy or to product them against cybercrimes such as personal identity theft. Attribute based encryption is one of the most attractive way to manage and control file sharing in cloud with its special attribute-Based Encryption have been proposed recently. To avoid fine-grained and scalable data access control for PHRs, Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file.

In quantum cryptography, Quantum Key Distribution Protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. Data configuration will not be possible here. However, public discussions require additional communication rounds between a sender and receiver and cost precious quits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication only. KEY distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication i+ possible on insecure public networks. However, various security problems exist in poorly designed key distribution protocols; for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority. This method having various drawbacks in storage security and data acquisition techniques.

Priyadharshini P, PG scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India. (Email: priyadharshinip2@gmail.com)

Revathi M, Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India

II. VARIOUS ATTRIBUTE-BASED ENCRYPTION (ABE) METHODS

Table 1 Analysis of Attribute-Based Encryption (ABE) methods

S.No	Title	Description
1	Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing[1]	In this technique cloud data storage is that of data integrity verification at un trusted servers. And proposed a general formal PoR model with public verifiability for cloud data storage, in which block less verification is achieved. It's supporting dynamic data operation for cloud data storage applications.
2	Privacy-Preserving Public Auditing for Secure Cloud Storage[2]	In [2], it is described that public auditing system of data storage security in Cloud Computing provides a privacy-preserving audit protocol. Its proposed an efficient approach based on probabilistic query and periodic verification for improving the performance

		of audit services.
3	Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds[3]	In this method, for cloud service providers to offer an efficient audit service to check the integrity and availability of the stored data. This approach based on probabilistic query and periodic verification.
4	Multi-user Dynamic Proofs of Data Possession using Trusted Hardware[4]	In [4], it is described that Dynamic Provable Data Possession (DPDP) work. The ability of users to access their data from anywhere, on a wide variety of devices. Challenges are convenient way to increase throughput for a complete remote storage solution such as the bulk storage server.
5	Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data[5]	In third-party sites on internet more sensitive data is shared and stored. We develop new cryptosystems (KP-ABE) Key-Policy Attribute-Based Encryption And Hierarchical Identity-Based Encryption (HIBE). Its provides sharing of audit-log information And broadcast encryption. The current constructions do not hide the set of attributes under which the data is encrypted.
6	Multi-authority attribute based encryption with honest-but-curious central authority[6]	In [6], it is described that Attribute based encryption. The proposed scheme, relies on the Bilinear Diffie-Hellman assumption. It is proved that our scheme is secure in the selective ID model and can tolerate an honest-but-curious central authority.
7	Decentralizing Attribute-Based Encryption[7]	This method for Multi-Authority Attribute-Based Encryption (ABE) system.We proves our system secure using the recent dual system encryption methodology. The challenge of proposed system is that multiple authorities who do not coordinate with each other introduce technical difficulties.
8	Attribute-Based Encryption with Fast Decryption[8]	Attribute-based encryption (ABE) is a public key encryption that allows users to encrypt and decrypt messages based on user attributes. Finally, tells a cipher text-policy ABE setting at a higher cost.
9	Attribute-Based Content Distribution with Hidden Policy[9]	In this paper we discuss about Access control in content distribution networks (CDNs). The recent CDNs usually resort to cryptographic-based distributed approaches. This approach provides flexible yet fine-grained access control (per file level) so that the contents are available only to the authorized users. An important future work is to implement our protocol and evaluate its practical performance.
10	Attribute Based Data Sharing with Attribute Revocation[10]	The Cipher text-Policy Attribute Based Encryption (CP-ABE) is for a fine-grained access control of shared data. We deals an important issue of attribute revocation. Its overcome by uniquely integrating the technique of proxy re-encryption with CP-ABE. Achieve this by uniquely integrating the technique of proxy re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to proxy servers. The future work is to combine a secure computation technique with our construction to guarantee the honesty of proxy servers.

III. CONCLUSION

In this paper, we studied about various attribute encryption techniques that identify the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained manner. Our security analysis tells that both *AnonyControl* and *AnonyControl-F* are secure under the decisional bilinear Diffie–Hellman assumption.

REFERENCES

[1] Enabling PublicVerifiability and Data Dynamic for Storage Security in CloudComputing. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling PublicVerifiability and Data Dynamic for Storage Security in CloudComputing," inthe Proceedings of ESORICS 2009.Springer-Verlag,2009, pp. 355–370.

[2] Privacy-Preserving Public Auditing forSecure Cloud Storage C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"in the Proceedings of IEEE INFOCOM 2010,2010,pp.525–533.

[3] Dynamic Audit Services for Integrity Verificationof Outsourced Storages in Clouds Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "DynamicAudit Services for Integrity Verification of Outsourced StorageinClouds," in the Proceedings of ACM SAC 2011,2011,pp.1550–1557.

[4] Multi-user Dynamic Proofs of Data Possession usingTrusted Hardware S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware," in Proceedings of ACMCODASPY'13,2013,pp.353–364.

[5] 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.

[6] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, "Multi-authority attribute-based encryption with honest-but-curious central authority," *Int. J. Comput. Math.*, vol. 89, no. 3, pp. 268–283, 2012.

[7] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2011,pp. 568–588.

[8] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in *Public-Key Cryptography*. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[9] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in *Proc. 4th Workshop Secure Netw. Protocols*, Oct. 2008, pp. 39–44.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. 5th ASIACCS*, 2010, pp. 261–270.