ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

A SURVEY PAPER ON CLOUD SECURITY WITH ANONYMOUS AUTHENTICATION OF DATA USING ABE

Atna Rose
B.Tech, Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India – 680307
atnarose@gmail.com

Deenrose Dickson
B.Tech, Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India – 680307
deenrose95@gmail.com

Anu KT
B.Tech, Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India – 680307
anumariya1120@gmail.com

Diana Poulose
B.Tech, Sahrdaya College of Engineering and Technology
Thrissur, Kerala, India – 680307
me.dayana.72@gmail.com

Abstract
This paper is a survey on decentralized access control plan for secure information storing in cloud which uses anonymous authentication. The cloud checks the genuineness of the content without knowing the client's identity before storing the data in cloud. This scheme consists of an additional feature called access control. In access control, only those users who are permitted can decrypt the data/information. This plan avoids replay attacks and additionally supports creation, modification, and reading the data which is stored in cloud. These schemes also address user revocation. Moreover, the access control scheme and authentication is decentralized and robust unlike any other access control schemes designed for clouds which are centralized. The communication, storage overheads and computation are comparable to centralized approaches.
Keywords— Access control, authentication, multi-authority, encryption, cloud storage.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

I. INTRODUCTION

In cloud computing, users can contract out their computation and storage to servers (also called clouds) using Internet. This frees users from the hardness of maintaining resources on-site. Several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms (e.g., Amazon's S3, Windows Azure).A lot of the information stored in clouds is very sensitive. At first step the user should authenticate itself before starting any transaction, and on the second step, it must be ensured that the cloud does not change the data that is outsourced.

User privacy is also required in cloud. By making use of privacy, the cloud or other users do not know the identity of the other users. The cloud can hold the user accounts for the data in cloud, and to provide services the cloud itself is accountable for. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy.

The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption [10], [11]. The problem here is that the data records should have keywords associated with them to enable the search. The correct records are returned only when searched with the exact keywords.

Security and privacy protection in clouds are being explored by many researchers. Wang et al. [12] addressed storage security using Reed-Solomon erasure-correcting codes. Authentication of users using public key cryptographic techniques has been studied in [10]. Many homomorphic encryption techniques have been suggested [13], [14] to ensure that the cloud is not able to read the data while performing computations on them.

II. METHODOLOGY

In [1], IBE scheme is used, a user has a set of attributes along with its unique ID. A Fuzzy IBE scheme can be applied to enable encryption. In Fuzzy scheme usually biometric input is used as identity. It allows error-tolerance between the identity of a private key and the public key used to encrypt a cipher-text. We described two practical applications of Fuzzy-IBE of encryption using biometrics and attribute-based encryption.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

Advantages:-

- Error-tolerant.
- Secure against attacks on collusion.

In [2], the sender has an authorization to encrypt information. Revoked attributes and keys of users cannot write again to store information. The attribute authority receives secret keys and attributes from the receiver and he/she is able to decrypt the data if it has matching attributes. This construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

Advantages:-

- Audit-log information is available to only authorized people and other than audit-log information no other information is provided.

In [3], the receiver has the access policy in the form of a tree. The tree contain leaves as its atuttribes and monotonic access structure with AND, OR and other threshold gates. Here, access policy, specified by the encryptor. This scheme is very expressive and provably secure under the decisional Bilinear Diffie-Hellman assumption.

Advantages:-

- Encrypted data can be kept confidential even if the storage server is untrusted.

In [4], a scheme is used in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext. Sahai and Waters introduced a single authority attribute encryption scheme and left open the question of whether a scheme could be constructed in which multiple authorities were allowed to distribute attributes [SW05].

Advantages:-

- Allows a more number of attributes.

In [5], users could have zero or more attributes from each authority and does not require a trusted server. Any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A user can encrypt data in terms of any boolean formula over attributes issued from any chosen set of authorities.

Advantages

- Collusion resistant.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

In [6], the paper subcontract the decryption task to a proxy server, so that the user could make computation on minimum resources like hand held devices. propose a new paradigm for ABE that largely eliminates this overhead for users. The paper shows how a user can provide the cloud with a single transformation key that allows the cloud to translate any ciphertext satisfied by that user's attributes into a El Gamal-style ciphertex

Advantages:-

- The user significantly saves bandwidth, without raising the number of transmission.

In [7], ABSs were introduced to ensure anonymous user authentication. This also used a centralized approach. formally define the security requirements of ABS as a cryptographic primitive, and then describe an efficient ABS construction based on groups with bilinear pairings. We prove that our construction is secure in the generic group model.

Advantages

- The user significantly saves decryption time, without raising the number of transmissions

In [8], it makes use of a decentralized approach and provides authentication without disclosing the identity of the users. It gives a general framework for constructing ABS schemes, and then show several practical instantiations based on groups with bilinear pairing operations, under standard assumptions.

Advantages:-

- Secure against a malicious attribute authority

In [10], fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails.

Advantages:-

- Uses an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads.

In [11], it allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

Advantages:-

- Highly efficient and resilient against malicious data modification attack, and even server colluding attacks.

III. DRAWBACKS

1. [1][2][3], in all these approaches, they take a centralized approach and allow only one KDC. The KDC is a single point of failure.
2. [4][5], in all these approaches, decryption at user's end is computation intensive. So, these techniques might be quite ineffective when users access using their mobile or handheld devices.
3. [6], in this scheme the presence of one proxy and one KDC makes it less useful than decentralized approaches. Together these approaches had no way to validate users, anonymously.
4. [7][8], these schemes are prone to replay attack.
5. [10][11][12], while providing efficient cross server storage verification and data availability insurance, these schemes are all focusing on static or archival data

IV. CONCLUSION

In this survey paper, the above discussed systems make use of centralized scheme that are prone to replay attacks. Decryption at user's end is computation intensive. So, these techniques might be quite ineffective when users access cloud using their mobile or handheld devices. Whereas, as a future vision to override the drawbacks found in the current system, even though the cloud does not know the identity of the user who stores the information, it can verify the user's credentials before the user puts the data in the cloud. Decentralized access control makes sure that only the valid users are allowed to decrypt the information stored in the cloud. Also, the system uses attribute-based encryption method for encrypting the data that is to be stored in the cloud.

ACKNOWLEDGMENT

We would like to take this opportunity to thank our project guide who helped us with all our doubts and involved in active discussion at all times. We would also like to thank our HOD for giving us an opportunity to work on the project. Also, we thank the staff members of Sahrdaya College of Engineering and Technology for the help provided by them.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 3, Issue 6, September 2016

REFERENCES

1. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
2. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption" Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
4. M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
5. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
6. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.
7. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
8. H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures" Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.
9. Sushmita Ruj, Member, Ieee, Milos Stojmenovic, Member, Ieee, And Amiya Nayak", Decentralized Access Control With Anonymous Authentication Of Data Stored In Clouds" Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.
10. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing", Proc. IEEE INFOCOM, pp. 441-445, 2010.
11. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136- 149, 2010.
12. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.
13. C. Gentry, "A Fully Homomorphic Encryption Scheme," PhDdissertation, Stanford Univ., http:// www.crypto.stanford.edu/ craig, 2009.
14. A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-BasednCloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.
15. R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http:// www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.
16. J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, pp. 1214-1221, July 2011.
17. A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.