Preserving Security and Privacy in cloud for Multi-owner data

[1] K.Manikandan Assistant professor Sri Guru Institute of Technology

[2] R.Malar Priya PG Scholar Adithya Institute of Technology

[3] M.Murugesan PG Scholar Sri Guru Institute of Technology

Abstract

Cloud Computing could be used almost everywhere in today's society and provides numerous benefits to companies, government and individual users. One main concern of using the cloud is data privacy and security especially for users with sensitive data that would be detrimental to the client if it were stolen. Sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper we use a digital group signature and broadcast encryption technique to provide a confidentiality, integrity, availability, accountability and privacy in multi-owner data.

Index Terms-cloud computing, dynamic group, access control, confidentiality, integrity, availability, accountability, privacy.

1. Introduction

Cloud computing is about moving services, computation and/or data—for cost and business advantage—off-site to an internal or external, location-transparent, centralized facility or contractor. By making data available in the cloud, it can be more easily and ubiquitously accessed, often at much lower cost, increasing its value by enabling opportunities for enhanced collaboration, integration, and analysis on a shared common platform.

A traditional data center of an organization is under

complete control of that organization. The organization logically and physically protects the data it owns. For economical reasons, an organization may choose to use a public cloud for hosting its business services. In this case, the organization loses control of its data. This poses critical security risks that the organization needs to carefully consider and mitigate.

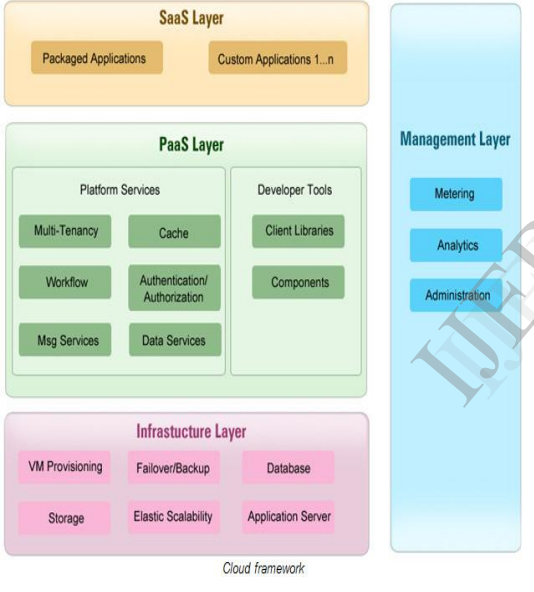

Fig1.Cloud Framework

The severity of risks depends on the sensitivity of the data stored in the cloud. Informal blogs twitter posts, public news, and newsgroup messages are examples of less sensitive data. The risk of hosting such data in the cloud is low. On the contrary, data such as health-related records, criminal records, credit history, and payroll information is highly sensitive business data. There are serious business and legal ramifications if such data is compromised. Therefore, the risk of hosting such data in the cloud is very high.

Since data in the cloud is physically in control of the cloud provider, the foremost risk is that of ensuring confidentiality of the stored data. Encryption can be employed to ensure confidentiality. If the cloud provider uses multi-tenancy architecture, then separate encryption keys, one per cloud consumer, should be employed.

Although cloud computing can offer small businesses significant cost-saving benefits—namely, pay-as-you-go access to sophisticated software and powerful hardware—the service does come with certain security risks. When evaluating potential providers of cloud-based services, you should keep these top six security concerns in mind.

i. Secure data transfer
ii. Secure software interfaces
iii. Secure stored data
iv. User access control

v. Data separation
vi. Multi authority Data

2. Literature Survey:

In Cloud Computing there are many threats which are avoiding the wide acceptance of cloud as explained above. The first problem with privacy is the disclosure of sensitive private information when exchanging data through the cloud service. And the sensitive private information includes: Personally identifiable information, Usage data, unique device identities and so on. The second problem is that people getting inappropriate or unauthorized access to personal data in the cloud by taking advantage of certain vulnerabilities, such as lack of access control enforcement, security holes and so on [6]. The third problem is that: because the feature of cloud computing is that it is a dynamic environment, in that service interactions can be created in a more dynamic way than traditional e-commerce scenarios. Services can potentially be aggregated and changed dynamically by service providers can change the provisioning of services. In such scenarios, personal
Sensitive data may move around within an organization or across organizational boundaries, so adequate protection of this information must be maintained despite the changes.

There is lot of research going on in this field to ensure and provide data integrity in cloud storages. A lot of research discuss this problem and introduce many solutions to decrease the threat of the data privacy and integrity. Priya Metri and Geeta Sarote [4] introduce threat model to treat the privacy problem in the clouds. One of the threats in cloud computing is tampering with data in the cloud that interfere with the unauthorized modifications for the data, which lead to an effectiveness on processors, data storage and data flow. Then, they suggested different solutions technique for this threat. One of the solutions is using digital signature which will be used in our model.

3 DESIGNS:

3.1 RSA Digital Signatures

The notion of digital signatures goes back to the beginning of public-key cryptography. In their landmark paper "New Directions for Cryptography" (*IEEE Transactions on Information Theory*, 1976), Whitfield Diffie and Martin Hellman introduced the idea that someone could form a digital signature using public-key cryptography that anyone else could verify but which no one else could generate.

While Diffie and Hellman provided a general model for digital signatures of any kind, the method developed by Rivest, Shamir, and Adleman in 1977, known as "RSA," has become the most proven and most popular, and achieved the widest adoption by standards bodies and in practice. Two other methods, discrete logarithm cryptography (including the Digital Signature Algorithm and the Diffie-Hellman key agreement method) and elliptic curve cryptography (see "Elliptic Curves and Cryptography," by Aleksandar Jurisic and Alfred J. Menezes, *DDJ*, April 1997) have also been embodied in several standards, but neither has yet been as widely adopted in practice as RSA.

The RSA digital signature scheme applies the sender's private key to a message to generate a signature. The signature can then be verified by applying the corresponding public key to the message and the signature through the verification process, providing either a valid or invalid result. These two operations — *sign* and v*erify* — comprise the RSA digital signature scheme.

Any signature generated by the first operation will always verify correctly with the second operation if the corresponding public key is used. If the signature was generated differently or if the message was altered after being signed, then the chances of the second operation verifying correctly are extremely small; with typical parameters, the chance is roughly 1 in 2160 or essentially zero. Although there are better ways to forge a signature than just guessing, the use of a sufficiently

large key ensures security by making it computationally impractical to do so. For instance, it has been estimated to take thousands or even millions of years to break a given 1024-bit key (find the private key, given the public key), depending on the amount of computing power applied.

Taking a closer look at the signature generation portion of the process, the first step in generating an RSA signature is applying a cryptographic hash function to the message. The hash function is specifically designed to reduce a message of any length to a short number, called the "hash value" (typically 160 bits long), and to do it in a way such that two conditions are satisfied:

It is difficult to find a message with a specific hash value.

It is difficult to find two messages with the same hash value (an easier problem to solve).

While many hash functions are available, only a few are commonly used in practice.

Next, the hash value is converted into an integer called the "message representative," with a length that is the same as the length of the RSA key being employed. This is done by applying a padding format to the resulting hash value or embedding the hash value to produce the message representative. In addition to its length-matching function, the padding format also provides additional security and is the primary differentiator among the various RSA signature schemes.

The final step applies the RSA signature primitive to the message representative using the RSA private key to generate the signature.

3.2 BROADCAST Encryption

A broadcast scheme allocates keys to users so that given a subset of, the center can broadcast messages to all users following which all members of have a common key. A broadcast scheme is called resilient to a set if for every subset that does not intersect with, no eavesdropper, that has all secrets associated with members of, can obtain “knowledge” of the secret common to. Knowledge here can have two different interpretations:

The secret common to has some a-priori distribution (usually the uniform distribution) and given the keys of and the message transmitted by the center the conditional distribution of the secret is not changed. The secret of is pseudo-random, i.e. no computationally bounded (by probabilistic polynomial time) eavesdropper can distinguish between the secret and a truly random string; even if the eavesdropper is provided with the keys of the coalition the secret of remains pseudorandom.

Advantage of the scheme is that if the adversary is in fact successful, after collecting 100,000 decryption devices, and if we have captured one of the adversary eavesdropping devices, all is not lost. It is still a relatively simple matter to disable all adversary de vices by disabling one group of 1000 users, splitting these users amongst other groups; the adversary effort has been in vain.

4. PERFORMANCE

RSA Digital Signature is more secure than DSA and Elliptic curve Signature algorithm. Broadcast Encryption is more efficient than Multicast and unicast Transmission.

In fig2 X axis represent the encryption technique and Y axis represent the efficiency.

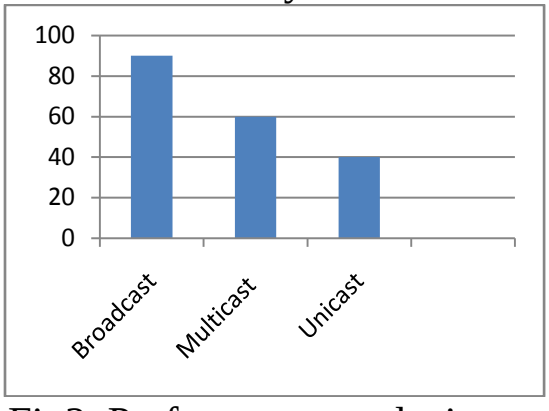

Fig2. Performance analysis

5. CONCLUSION

In this paper, we use a RSA digital signature and broadcast encryption to preserve confidentiality, integrity, availability, accountability and privacy in a multi-owner data.
A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it supports efficient user revocation and new user joining.

More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys

of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant.

6. REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" pp .1182-1191, Jun 2013.

[2] Zhifeng Xiao and Yang Xiao," Security and Privacy in Cloud Computing" pp.843-856, 2013.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed

Systems Security Symp. (NDSS), pp. 29-43, 2005.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[10] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[11] V. 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 (CCS), pp. 89-98, 2006.

[12] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[14] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[15] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.