ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Proxy Re-encryption Schemes for Data Security in Cloud

Rutuja Warhade[1]
PG Student
Dept. of Computer Engineering
GSMCOE
Pune – India

Prof. Basha Vankudothu[2]
Professor
Dept. of Computer Engineering
GSMCOE
Pune – India

Abstract: Cloud computing is an emerging technology in which resources of the computing infrastructures are provided as services of the internet. Cloud allows user to access application without installation and their personal data at any computer with internet access. It provides with a way to share distributed recourses and services that belong to different organizations or sites. In this technology users have to entrust their data to cloud providers, there are several security and privacy concerns on outsourced data. As the data is shared over the network, the data should be encrypted to maintain confidentiality against untrusted users. There are various encryption schemes that provide security and access control over the network. A main emphasis of this paper is on the data encryption techniques like proxy re-encryption and many more.

Keywords: Cloud computing; encryption; proxy re-encryption; data confidentiality; Proxy re-encryption techniques.

I. INTRODUCTION

The cloud computing is an internet-based computing technology, where customer can share the resources such as software, platform, storage and information as per their demand. In cloud computing customers information and data are stored on distributed servers at remote location. The remote locations are known as 'data centers'. The client can purchase or rent, such as network bandwidth, memory etc as per their business requirements. Customers can distantly store their data in the cloud and no longer posses the data locally. Cloud computing moves the application software and database to the large data center, where the data management and data security may not be fully trustworthy [3].

A cloud storage system is a distributed storage system [2], which consists of many independent storage servers. The purpose of distributed storage systems is to store data reliably over long periods of time [1]. The main aspect of cloud computing is that many enterprise application are moving into cloud services. The data stored in the cloud is accessed a large number of times and is often subject to different types of changes. An important aspect of cloud storage servers is that, it gives rise to a number of security threats.

Cloud services and applications should follow the standard security measures including data confidentiality, integrity, privacy, robustness and access control. Hence providing security to the cloud is the challenging task. There are various cryptographic methods to secure the data in cloud storage systems. In these paper encryption techniques such as proxy re-encryption (PRE) scheme, Type based PRE, Key-private PRE, Identity based PRE, Attribute based PRE and Threshold PRE are discussed. The paper has been organized as follows. In section II cloud architecture is discussed. In section III the Proxy re-encryption techniques are discussed. Finally In section IV, the conclusion and future work is presented.

II. Cloud Architecture

The cloud computing system can broadly divided into two sections: the **front end** and the **back end**. The two sections connect to each other through the Internet. The front end is the user side or the section which computer user, or client, sees. The "cloud storage" section is the back end of the system. The cloud computing architecture consists of many cloud components, each of this components are loosely coupled. The typical cloud architecture is illustrated in Fig 1.

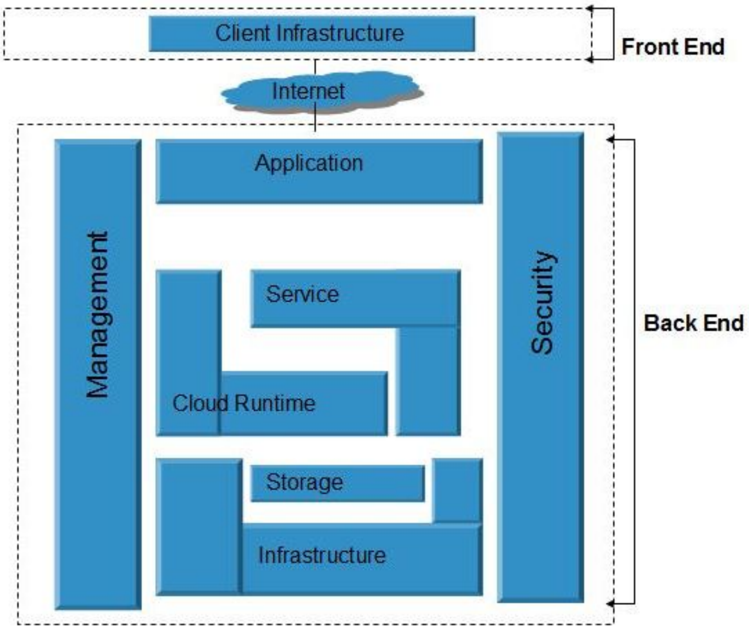

Fig 1. The Cloud Architecture

The front end comprises of the client infrastructure that includes the client's computer and some application that are necessary to connect the client to the remote cloud server. Identical user interface are used by all the cloud-computing systems. They provide Services like Web-based e-mail programs leverage, which employs Internet Explorer or Fire fox types of Web browsers. Other systems have exclusive applications that offer network access to clients [4].

Moreover the cloud of a computer services is created on the back end of the system with the help of various computers, servers and data storage systems. In general, a cloud computing system could include almost any computer program you can imagine ranging from data processing to video games. Usually, each application is govern by its own dedicated server.

In order to run everything smoothly a central server administers the system is employed that monitoring traffic and client demand and ensures that the process is smooth enough. It employs some a set of rules called **protocols** and also bring in use a special kind of software called **middleware**. Middleware basically allows networked computers to establish communicate among computers. Maximum number of time it is seen that servers don't run at full capacity. That means that the power is not used to its fullest extend and the unused processing power is wasted. It's possible to fool a physical server to think that but it is actually multiple servers, each operating with its own self-governing operating system. This technique is popularly known as server virtualization. Server virtualization reduces the need for more physical machines by maximizing the output of individual servers. If there are a lot of clients in a cloud computing company then there's likely to be a high demand for a lot of storage space

As cloud system requires at least twice the of storage device. This is because if there is a break down in the cloud computing system, then the system should be able to recover the data. For this reason it is needed to create copies of data that should be stored as a backup, which can be retrieved whenever needed. Creating these backup copies is known as **redundancy**.

III. Proxy Re-Encryption Technology

A vital approach for secure data sharing in a cloud environment is to let the data owner encrypt data. To achieve a combination of fine-grained access control on encrypted data as well as scalable user revocation attribute-based encryption (ABE) and proxy re-encryption (PRE) to delegate the cloud service provider (CSP) to execute re-encryption. In order to send the PRE keys to the CSP in a timely fashion the data holder should be online, so the revoked user can be prevent from accessing the forthcoming data. Potential security risks due to the delay involved in issuing the PRE keys.

A. Proxy Re-encryption Scheme

In paper [5] the author's discus the proxy re-encryption from both a theoretical and practical viewpoint. The authors summarize the characteristics and security issues of formerly known schemes, and compared them to a suite of improved re-encryption schemes that is present over bilinear maps. Due to the implementation of pairing-based schemes important new features, such as protection the master secret key of the delegator from a colluding proxy and delegate are obtained giving proxy capabilities to the key server of a confidential distributed file system was one of the most promising applications for proxy re-encryption is; this way the key server need not be fully trusted with all the keys of the system and the secret storage for each user can also be reduced. This paper employs this idea in the context of the Chefs file system, and showed experimentally that enhances security benefits of proxy re-encryption that it can be obtained for a manageable amount of run-time overhead.

The main contribution of paper [6] is that it dignifies the definitions of the bidirectional and unidirectional proxy *functions* for encryption and signatures and their security guarantees. In addition, for each class of proxy functions, the paper describes one generic technique and several specific techniques to transform a standard cryptographic primitive into a proxy function

B. Type Based Proxy Re-encryption Scheme

Recently, in several applications the concept of proxy re-encryption has been shown very useful, especially in the ones where imposing access control policies are employed. In present proxy re-encryption schemes, the delegate can decrypt all cipher texts for the delegator after re-encryption by the proxy. Therefore, in order to employ a fine-grained access control policies, where the delegator needs to either implement multiple key pairs or trust the proxy to behave honestly.

Another author [7], extends this concept and proposes type-based proxy re-encryption, which allows the delegator to selectively delegate his decryption right to the delegate though only needs one key pair. As a consequence, type-based proxy re-encryption permits the delegator to use fine-grained policies merely with one key pair deprived of any additional trust on the proxy. The system also provides a security model for our conceptual knowledge and provides proper definitions for semantic security and cipher text privacy, which is an important attribute in privacy-sensitive circumstances. It also provides two type-based proxy re-encryption schemes: one is CPA secure with cipher text privacy while the other is CCA secure without cipher text privacy.

C. Key Private Proxy Re-encryption Scheme

In many applications, to protect data with one public key pk1 requires to be disseminated to every user with a unique public key pk2. This becomes little impractical for the owner of sk1 to be online to decrypt these cipher texts and then encrypt these contents under a new key pk2. For example, Lisa might wish to have her mail server forward her encrypted email to john while she is on vacation. However, how can Lisa do this without telling her sk1 to either her mail server or John? As solution to this key management problem, the concept of proxy re-encryption (PRE) was introduced

In a research [8] the author proposes a key-private (or anonymous) re-encryption keys as an additional property that enhances the PRE schemes, the authors defines PRE scheme to be secure and key-private. Unexpectedly, the system show that this property is not achieved by previous schemes, also even after including the secure the communication from being harder to interpret PRE by Hohenberger et al. (TCC 2007). Finally, the author conclude by proposing one of the unique feature of the first key-private PRE construction and prove its CPA-security under a simple extension of Decisional Bilinear Diffe Hellman assumption and its key-privacy under the Decision Linear assumption in the standard model.

D. Re-encryption Scheme

In Identity-Based Encryption (IBE) use of public key certificate is avoided instead a sender is allow to encrypt a message to an identity. The ability to perform public key encryption without using certificates has several practical applications. Let's consider an example, a user can transmit an encrypted mail to a recipient, e.g. johnsmith@gmail.com, without requiring either the existence of a Public-Key Infrastructure or that the recipient be on-line at the time of establishment connection. One common feature of all previous Identity-Based Encryption systems is that they consider identities as characters of string.

An author in his research work proposes a new type of Identity-Based Encryption known as Fuzzy Identity-Based Encryption [9] in which the identities are considered to be a set of descriptive attributes. According to the Fuzzy Identity-Based Encryption scheme, a user with the undisclosed key for the identity ω is able to decrypt a cipher text encrypted with the public key ω 0 if and merely if ω and ω 0 are inside a definite distance from each other as estimated by some metric. So, the system allows for a certain amount of error-tolerance in the identities.

In this paper [10] the author puts light on a problem faced by Identity-Based proxy re-encryption. The problem related to the IBE was the cipher texts were changed from one identity to another. The schemes are compatible with current IBE deployments and do not require any extra work from the IBE trusted-party key generator. Moreover, they are non-interactive and some of them also allow multiple re-encryptions. Their security is based on a standard supposition (DBDH) in the random oracle model.

In [11] proposes a complete functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming an elliptic curve variant of the computational Diffe-Hellman problem. The system is mainly based on the Weil pairing. It also gives precise definition for secure identity based encryption schemes and gives several applications for such systems.

E. Attribute Based Proxy Re-encryption Scheme

In an ABE system, if there is a match between the attributes of the ciphertext and the user's key then a user's keys and ciphertexts are labelled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext. Some researchers propose cryptosystem, which allows decryption when at least k attributes overlapped between a ciphertext and a private key. Even though this primitive was practical proven useful for error-tolerant encryption with biometrics, they seem to limit its applicability to larger systems due to the lack of expressibility.

According to [12] a novel system was developed a new cryptosystem for fine-grained sharing of encrypted data that is known as Key-Policy Attribute-Based Encryption (KP-ABE). Moreover the cryptosystem, in order to control on which ciphertexts a user is able to decrypt depends on the ciphertexts which are labelled with sets of attributes and private keys are associated with access structures. The system exhibits the applicability of our construction to sharing of audit-log information and broadcast encryption. Also the construction supports delegation of private keys, which subsumes Hierarchical Identity-Based Encryption (HIBE).

F. Conditional Proxy Re-encryption Scheme

Proxy re-encryption can be used in applications where delegation is required, for an example in case of delegated email processing. But, it is not enough to handle scenarios where a fine-grained delegation is demanded. For example, john is only allowed Lisa's encrypted emails containing a predetermine keyword. In order to overcome the limitation of existing PRE, in [13] the system introduces the notion of conditional proxy re-encryption (or C-PRE), whereby only ciphertext satisfying one condition set by Alice can be transformed by the proxy and then decrypted by john. The author formulates its security model and also proposes an efficient C-PRE scheme, whose chosen-ciphertext security is proven under the 3-quotient bilinear Diffe-Hellman assumption. The author further extends the structure, which allows multiple conditions with a somewhat high overhead.

G. Time Based Proxy Re-encryption Scheme

In paper, author proposed the Time based PRE scheme to achieve fine-grained access control and scalable user revocation in a cloud environment [14]. The scheme allows every user's access right to be effectual in a pre-determined time period, and enables the CSP to re-encrypt ciphertexts automatically, based on its own time. This allows data owner to be offline in the process of user revocations. The main disadvantage of the scheme is that it requires the effective time periods to be the same for all attributes associated with a user. Although the author provides a probable enhancement, the users will be issued more UAKs. Our future work is to allow different effective time periods for different attributes associated with a user, without increasing the number of UAKs associated with each user.

H. Threshold Proxy Re-encryption Scheme

The authors propose a method known as threshold proxy re-encryption scheme [15]. In order to formulate a secure distributed storage system the scheme is integrated with a decentralized erasure code. This system not only supports storing and retrieving in secure manner, but it also provides message forwarding from server to server without retrieving. The technique employed here mainly concentrate on encoding the encrypted message, its forwarding methods and even its decryption. The system allows more flexibility as it provides copy of robustness data in all storage servers.

In the proposed system a secure distributed storage system is formulated by integrating a threshold proxy re-encryption scheme with a decentralized erasure code [16]. The distributed storage system not only provides secure and robust data storage and recovery, but also allows a user to forward data from one user to another user without retrieving the data back. The major technical involvement is that the proxy re-encryption scheme supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. The technique is completely integrates encrypting, encoding, and forwarding. The proposed system is applied for military and hospital applications and also for other secret data transmissions.

IV. CONCLUSION

In this paper, we conducted a survey on different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with access to non-monotonic structure, HABE and MA-ABE .The main access polices are KP-ABE and CP-ABE, moreover the schemes obtained are based on these policies. Depending on their type of access structure the schemes are classified as either monotonic or non-monotonic.

References

1. A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J.Wainwright, and K. Ramchandran "Network coding for distributed storage systems", IEEE, 2010,pp. 4539-4551.
2. P. Druschel and A. Rowstron,"PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility", Proc.Eighth Workshop Hot Topics in Operating System, 2001, pp. 75-80.
3. C.Wang, QianWang, KuiRen, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", Proc. IWQoS 09, July 2009, pp.1–9.
4. http://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm
5. Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage" Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS), February 2005, and a journal version has been accepted for publication in ACM Transactions on Information and System Security (TISSEC).
6. Anca Ivan, Yevgeniy Dodis "Proxy Cryptography Revisited"
7. Giuseppe Ateniese, Karyn Benson, Susan Hohenberger "Key-Private Proxy Re-Encryption"
8. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In ASIACRYPT, pages 566–582, 2001
9. Amit Sahai, Brent Waters, "Fuzzy Identity-Based Encryption"
10. Matthew Green, Giuseppe Ateniese "Identity-Based Proxy Re-Encryption."

11. D. Boneh and M. Franklin. Identity Based Encryption from the Weil Pairing. In Advances in Cryptology – CRYPTO, volume 2139 of LNCS, pages 213–229. Springer, 2001.

12. Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data."

13. B. Libert and D. Vergnaud. Tracing Malicious Proxies in Proxy Re-Encryption. In Proc. of Pairing'08, LNCS 5209, pp. 332-353, Springer-Verlag, 2008.

14. Qin Liu, Guojun Wang, Jie Wu, "Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment." Preprint submitted to Elsevier Information Sciences September 18, 2012

15. S.Amritha, Mr.S.Saravana Kumar, "Threshold Proxy Re-Encryption Scheme and Decentralized Erasure Code in Cloud Storage with Secure Data Forwarding." IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 5 (Mar. - Apr. 2013), PP 27-31 www.iosrjournals.org

AUTHOR(S) PROFILE

Rutuja Warhade, received the B.E. in Computer Science from Vishvesvaraya National Institute of Technology, Nagpur in May 2004. Currently she is perusing her M.E. in Computer Engineering from GSMCOE, Pune. She has more than five years of industrial experience in Web Technologies. Her research interests include Cloud computing security, Web Mining.

Basha Vankudothu, received the B.Tech in Computer science and engineering from JNTU Hyderabad, and M.Tech(C.S.E) from IIT Madras. Currently perusing Ph.D from JNTU Hyderabad. He has 6 years of teaching experience. Area of research interest is Mobile computing & Sensor Networks.