International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Re-encryption based Attribute Revocation in Data Access Control for Multi-Authority Cloud Storage

Kalyani G. Kotangale[1], Milind Penurkar[2]

[1]MITCOE Pune-38, Maharashtra, India

[2]Professor, MITCOE Pune-38, Maharashtra, India

Abstract: ***In Services including private users, businesses and governments, Cloud Computing technologies are gaining importance at a very higher level. Cloud computing provides transparency, but sharing of resources at a distributed level has severe implications when sensitive or privacy-relevant data is concerned. To ensure the data security in cloud Data access control is an effective way . But due to the untrusted cloud servers, data access contoll becomes a challenging issue in cloud storage systems . However after attribute revocation if we have to provide security through re-encryption, then this is not given .In this paper we proposed re-encryption-based attribute revocation schemes by relying on a trusted server and we apply it as underlying techniques to design the data access control scheme. Our re-encryption method can efficiently provide both forward security and backward security.***

Keywords: Data access control, Attribute Revocation , Re-encryption

1. Introduction

In cloud computing, security is the main important constraint which is only the main focus of this survey. Here the Encryption module, Decryption module, Splitter module and Joinner module are used to provide security at a higher level. Encryption is a technique where we change the original content with some code to provide security to the data. There is some private key is used to encrypt the data. Encrypted data can be re-encrypted again to provide higher level of security. During the decryption, with the help of the public key of owner we can get the decrypted data in original form to particular user, and hense security to the data is provided. Before encryption the original data is splitted into chunks with the help of Splitter module .And during Decryption all the decrypted chunks get joined together with the help of the Joinner module. Attribute revocation means to get or to revoke the original data which is encrypted. Multi-authority cloud storage means multiple users can use the data to store and download from the cloud .In such a way higher level of security is provided in cloud storage.

2. Literature Survey

1) Improving Privacy and Security in Multi-Authority Attribute-Based Encryption [1]

This paper proposed an attribute- based encryption scheme without the trusted authority, and an anonymous key issuing protocol. Authors ensured that their work give a more practice-oriented attribute based encryption system. Here author reviewed the motivation behind the use of the trusted central authority (CA) and how to avoid it.

Author also mentioned that in a multi-authority ABE scheme, different attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Authors studied a multi-authority ABE scheme using the concepts of a trusted central authority (CA) and global identifiers (GID) but the CA in that construction has the power to decrypt every ciphertext, which they found out contradictory to the original goal of distributing control over many potentially untrusted authorities. Also in that construction, the use of a consistent GID allowed the authorities to combine their information to build a profile with all of a user's attributes, which unnecessarily compromises the privacy of the user so authors proposed a method which removes the trusted central authority, and protects the users privacy by preventing the authorities from getting their information on particular users, thus making ABE more usable in practice.

2) Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage[2]

In this paper, author propoed an expressive, efficient and revocable data access control method for multi-authority cloud storage, where there are multiple authorities present and each authority can issue attributes independently. Author mentioned that data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Cipher text-Policy Attribute-based Encryption (CP - ABE) is considered as one of the most suitable methods for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP -ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. Specifically, Author proposed a revocable multi -authority CP- ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results how that our

proposed data access control scheme is secure in the random oracle mode and is more efficient than previous works.

3) An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing[3]

In this paper, authors first studied the problem of Confidentiality and Integrity of data storage in cloud computing and proposed an efficient and secure protocol using ECC and Sobol sequence. The proposed method is mainly suitable for thin users who have less resources and limited computing capability scheme also supports dynamic data operations. Proposed scheme satisfies the all security and performance requirements of cloud data storage. Our method also supports public verifiability that enables TPA to verify the integrity of data without retrieving original data from the server and probability detects data corruptions.

4) Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption[4]

In this paper, author proposed a novel patient-centric framework for data access control to Personal Health Records (PHRs) stored in semitrusted servers. To achieve scalable data access control for PHRs, author used attribute-based encryption (ABE) techniques to encrypt patient's PHR file. Author mainly focused on the multiple data owner scenario for data outsourcing and divides the users in the PHR system into multiple security domains that reduces the management complexity for owners and users.

Author first mentioned that although Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers but there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

Proposed method provides high degree of patient privacy and also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation. Author carried out extensive analytical and experimental results which showed the security, scalability, and efficiency of our proposed scheme.

5) Ensuring Data Storage Security in Cloud Computing[5]

In this paper, author proposed an effective distributed scheme with explicit dynamic data support to ensure the correctness of users data in the cloud. Author proposed data correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability which drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. This system uses homomorphic token with distributed verification of erasure-coded data.

Proposed system is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. Proposed system not only achieves the storage correctness insurance but also data error localization. The main disadvantage of this system is that anyone can intentionally access or modify the data because author does not used any encryption scheme.

3. Architecture Modules

1) **Encryption Module**
2) **Splitter Module**
3) **Decryption Module**
4) **Joiner Module**

1) Encryption Module

This module is important to encrypt the chunks of the splitted file, for future security

2) Splitter Module

This module is used to split the given file to protect.It splits the required file into no. of chunks

3) Decryption Module

This module decrypts all the encrypted chunks of the data for further to join and use it

4) Joiner Module

This module joins all the encrypted chunks to get the final image or a file to download for the user

4. Applications

- To provide security to data owner
- To provide Confidentiality, Integrity and Availability to user

5. Conclusion

In many organizations the main issues is maintaining the security and privacy of confidential data. Cloud store different types of data for example documents, data sheets, digital media object and it is necessary to give guarantee about data confidentiality. Data integrity, privacy are the terms which examines all stored data to maintain privacy and integrity of data and give data confidentiality.

References

[1] Kan Yang, and Xiaohua Jia, " Expressive, Efficient, and Revocable Data Access Control f or Multi-Authority Cloud Storage*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,*Vol.25, No.7, pp. 1735-1744, July 2014.

[2] Sherman S.M. Chow " Improving Privacy and Security in Multi-Authority Attribute-Based Encryption" *Melissa Chase Microsoft Research 1 Microsoft Way Redmond, WA 98052, USA melissac@microsoft.com Department of Computer Science Courant Institute of Mathematical Sciences New York University, NY 10012, USA schow@cs.nyu.edu 2013*

[3] " Ming Li, Member , IEEE, Shucheng Yu, Member , IEEE , Yao Zheng, Student Member , IEEE , Kui Ren, Senior Member , IEEE , and Wenjing Lou, Senior Member , IEEE "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013*

[4] Syam Kumar P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing*" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011*

[5] Cong Wang, Qian Wang, and Kui Ren Department of ECE Illinois Institute of Technology "Ensuring Data Storage Security in Cloud Computing" *Email: cwang, qwang, kren}@ece.iit.edu Wenjing Lou Department of ECE Worcester Polytechnic Institute Email: wjlou@ece.wpi.edu JULY 2012*