A SURVEY ON THRESHOLD CRYPTOGRAPHY BASED CLOUD DATA SECURITY

Ms. Paurnima Ghugarkar[1], Prof. Vrushali Ranmalkar[2]

[1] *Student, Computer Engineering, VACOE, Ahmednagar, Maharashtra, India*
[2] *Professor, Computer Engineering, VACOE, Ahmednagar, Maharashtra, India*

ABSTRACT

Recently cloud computing is very popular in organizations and institutions because it provides storage and computing services at very low cost. However, it also introduces new challenges for ensuring the confidentiality, access control and integrity of the data. Some approaches are given to ensure these security requirements but they are lacked in some ways such as violation of data confidentiality due to heavy computation and collusion attack. To address these issues we propose a scheme that uses threshold cryptography in which data owner divides users in groups and provides single key to every user group for decryption of data and, each user in the group shares parts of the key. In this paper, we use capability list to control the access. This system not only provides the strong data confidentiality but also reduces the number of keys.

Keywords: - *Authentication, access control, threshold cryptography, outsourced data, capability list, Malicious outsiders.*

1. INTRODUCTION

Cloud computing is a new and fast growing technology in field of storage computation of data. It provides storage and computing as a service at very attractive cost. Cloud computing can also be defined as a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or many unified computing resources based on service-level agreements established through negotiation between consumers and the service provider. In recent past, various commercial models are developed that are described by X as a Service (XaaS) where X could be hardware, software or storage etc. Successful examples of emerging cloud computing infrastructures are Microsoft Azure, Amazons EC2 and S3 [6], and Google App Engine etc.

It provides services according to three fundamental service models: platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS). Storage as a service is basically a platform as a service. The five characteristics of cloud computing are: on-demand service, self service, location independent, rapid elasticity and measured scale service. These characteristics make cloud significant. Cloud computing has become a necessity now era when an enterprise plans to increase its capacity or capabilities on the y without investing on new infrastructure, training new personnel, buying new software licenses etc. It encompasses any subscription-based or pay-per-use service that extends the enterprises existing IT capabilities, in real-time over the Internet. Industries and institutions are exploiting these characteristics of cloud computing and increasing their revenue and profit [1]. That is why, industries are shifting their businesses towards cloud computing.

However, data security is a major obstacle in the way of computing. People are still fearing to exploit the cloud computing. Some people believe that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it [2][3]. They are more or less right. Data of data owners are processed and stored at external servers. So, confidentiality, integrity and access of data become more vulnerable. Since external servers are operated by commercial service providers, data owner can't trust on them as they can use data for their benefits and can

destroy businesses of data owner [4]. Data owner even can't trust on users as they may be malicious. Data confidentiality may violet through collusion attack of malicious users and service providers. Many schemes are presented to ensure these security requirements but they are suffering from collusion attack of malicious users and cloud service provider and heavy computation (due to large no keys).

To address these problems we propose a scheme. In this scheme, there are basically three entities: Data Owner (DO), Cloud Service Provider (CSP) and Users. The data owner places the data on the CSP which the user wants to access. As the CSP is un-trusted, data owner places encrypted data on CSP. Upon receiving a data access request from the user, DO sends required a certificate and keys to the user. User then presents the certificate to CSP and gets the encrypted data upon successful verification by CSP. Users are divided in groups on some basis such as project, location and department and, corresponding to each group, there is a single key for encryption and decryption of data. Each user in the group shares parts of the key. Data can be decrypted when at least threshold no. of users will present. This scheme not only provides data confidentiality by all means but also reduces the number of keys. To accomplish fine-grained data access control, the approach has used capability list [5].

It is basically row-based decomposition of access matrix. In capability list operations and authorized data for a user are specified. It is better suit than Access Control List (ACL) [6][7][8] because ACL specifies users and their permitted operation for each data and file. It is practically inefficient that 2 users require same data and have same operations on it. In this paper, the approach has used the modified Diffie-Hellman algorithm to generate one time shared session-key between user and CSP to protect the data from outsiders. To ensure data integrity the approach has used MD5 [4].

2. LITRATURE SURVEY

Access control, data confidentiality are two basic security requirements for outsourced data in cloud computing. Sometime, when we emphasize more on security of data, we forget about performance of systems (CSP, DO, users). For example, to secure data, we sometime use too many keys. We know that keys are confidential, so there is need to secure and maintain these keys which are additional work. These works affect the performance of the system. So, it is desirable to reduce no of keys. So, there is need a scheme that provides not only data security but also maintain the performance. Many schemes are suggested to meet these requirements. The scheme proposed in [9] is the group-key scheme. In group-key scheme, there is a single key corresponding to every group of users for decryption process and all users of the group know that key. Here, number of keys is reduced but there is a problem of collusion attack of a user and cloud service provider because a single malicious user can leak whole data of the group to CSP. We know that CSP is not trusted party. It can use data owner's data for its commercial benefits.

The scheme proposed in [4.] tried to achieve access control and data confidentiality. In this scheme, data are encrypted by symmetric keys and symmetric keys are known only to data owner and corresponding data users. The encrypted data are stored at CSP. CSP cannot see data stored at it as data are encrypted. Data are further encrypted by one time secrete session-key shared between user and CSP by the modified Diffie-Hellman protocol to secure data from outsiders during the transmission between CSP and user. This scheme no doubt provides whole data security but there is associated a key corresponding to every user and users may be large in number in some applications. So, number of keys may increase. Hence, increases the maintenance and security concerns of keys.

Communication model of the proposed scheme somehow matches with it [4.] but proposed scheme is more secure and reduces number of keys. The proposed scheme is useful for those applications where works are done in group and team such as in software industries. You may think proposed scheme has limited applications but it is not as such. It is applicable all where you can group users on some basis and can apply threshold cryptography technique. Such as hardware and software industries, institutes, banks and medicals fields. There is provision of hierarchy of access in this scheme which makes this scheme more realistic and useful. For Example, university has vice-chancellor, hods, teachers, clerklier-staff and students. Each one has different level of access right.

2.1 Jeong-Min Do, "Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments"-

Key Policy-Attribute Based Encryption (KP-ABE) and Proxy Re-Encryption (PRE) are proposed to ensure access control and data confidentiality in cloud computing. But, these technologies affect the confidentiality of data through collusion attack of new user in system and cloud server. To recover this issue, a new system has been

proposed that store and divide data file into header, body. In addition, this scheme selectively delegates decryption right using Type-based Proxy re-encryption.

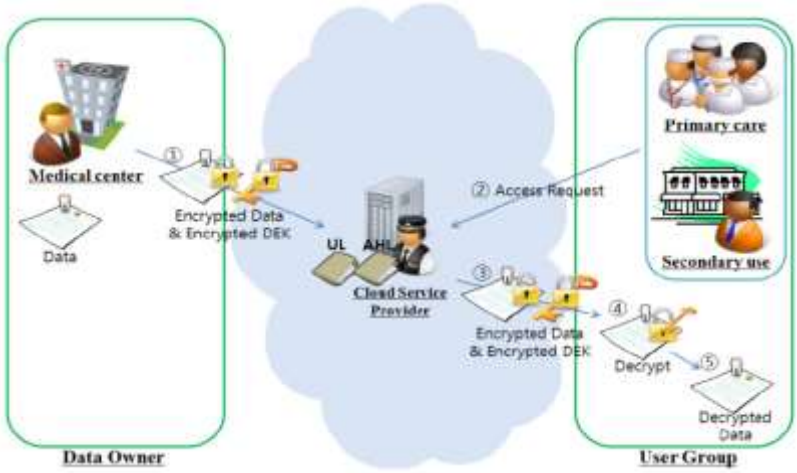

Fig -1: Architecture diagram

2.2 Adi Shamir, How to share a secret-

This paper proposes a schema which shows how to partition data into fragments in such way that it becomes very easy to reconstruct the original data from any partition, but even complete knowledge of k-1 fragments cannot help to get the whole information about D. This technique helps in construction of key management schemes which are strong for cryptographic system can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

2.3 Sunil Sanka, Secure Data Access in Cloud Computing-

Cloud computing is used by cloud users to outsource their sensitive and confidential data to CSPs which leads to carry out research work on data security and access control of that data. Some existing solutions that are proposed makes use cryptographic techniques to provide access control and data security problems but they increase the computational overhead on the data owner as well as the cloud service provider as they require to manage the keys as well as their distribution. In this section F, capability based access control technique is been proposed which ensures only authorized users will access the data stored on cloud. This work also designs a new modified version Diffie-Hellman key exchange protocol which is used between cloud service provider and the user for sharing a symmetric key secretly so as to facilitate authorized data access that will solve the issue of key management and its distribution at cloud service provider. The proposed approach is efficient and secure under existing security models.

2.4 Giuseppe Ateniese, Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage-

Blaze, Bleumer, and Strauss (BBS) proposed an application, in 1998, called as atomic proxy re-encryption. This application converts a cipher-text for Alice into a cipher-text for Bob without considering the plaintext using a semi-trusted proxy. It can be predicted that use of efficient and rapid re-encryption will become tremendously popular as a solution for dealing with encrypted file systems. The technique called as BBS re-encryption is mostly in use but, it has many security risks. Recent work done by Dodis and Ivan, present a new schemes for re-encryption that deals with efficient way to provide security and also delivers the way of providing access control to a file system security.

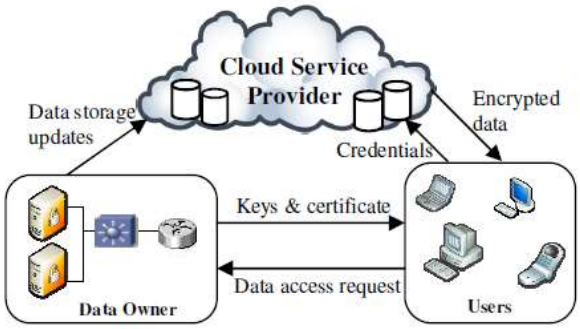

Fig - 2: Architecture diagram.

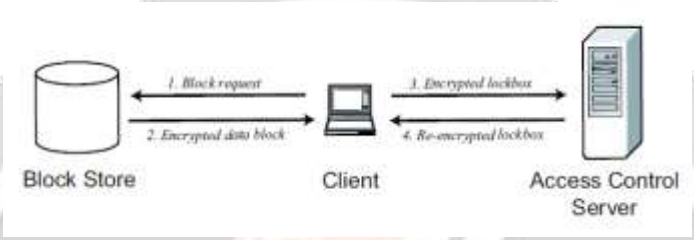

Fig - 3: Encryption of file.

2.5 Nadia Bennani, Toward cloud-based key management for outsourced databases-

A major drawback of implementing Database-as-a-Service (DaaS) on untrusted servers is the complexity of key management required for handling revocation. In this section we put forward the concept of using the cloud for decoupling the management of local, user- specific encryption keys from the one of role-specific protection keys, obtaining simple key management and revocation schemes.

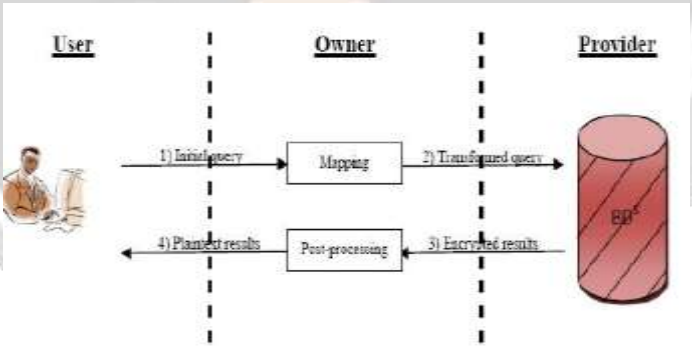

Fig - 4: Querying an outsourced database in the owner side policy enforcement.

2.6 Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing-

Cloud computing is an rising computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth more new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as DO. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The issue of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This section addresses this challenging open issue by, on one hand, enforcing and defining access policies based on data attributes, and, on the other hand, allowing the DO to delegate most of the computation

tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by uniquely combining and exploiting techniques of attribute-based encryption, lazy re-encryption and proxy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is provably secure and highly efficient under existing security models.

3. CONCLUSIONS

In this project, we presented a new approach which provides security for data outsourced at CSP. Some approaches are given to secure outsourced data but they are suffering from having huge number of keys and collusion attack. By employing the threshold cryptography at the user side, we secure outsourced data from collusion attack. Since, DO stores its data at cloud service provider in encrypted form and, keys are known only to DO and respected users group, data confidentiality is ensured. To ensure fine-grained access control of outsourced data, the scheme has used capability list. Public key cryptography and MD5 ensure the entity authentication and data integrity respectively. Public key cryptography and D-H exchange protected the data from outsiders in our approach. No of keys (because in threshold cryptography, there is a single key corresponding to each group) have reduced in the proposed scheme.

4. ACKNOWLEDGEMENT

The All faith and honor to the HOD for his grace and inspiration. I would like to thank all my Friends and Family members they were always been there to support me. I sincerely thanks to my Department Head, PG coordinator and all other staff members to give me the guidelines for this paper.

5. REFERENCES

[1] J.Do, Y.Song, and N.Park, "Attribute Based Proxy Re-encryption for Data Confidentiality in Cloud Computing Environments," Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on, vol., no., pp.248-251, 23-25 May 2011.

[2] T.Mather, S.Kumaraswamy, and S.Latif, "Cloud Security and Privacy," O'Reilly Media, Sep.2009.

[3] A.T.Velte, T.J.Velte, and R. Elsenpeter, "Cloud computing a practical approach," Tata McGraw-Hill Edition, 2010, ISBN- 3:978- 0-07-068351-8.

[4] S.Sanka, C.Hota, and M. Rajarajan, "Secure data access in cloud computing," Internet Multimedia Services Architecture and application (IMSAA), 2010 IEEE 4th International Conference on, vol. no., pp.1-6, 15-17 Dec.2010.

[5] C.Hota, S.Sanka, M. Rajarajan, and S.Nair, "Capability-Based Cryptographic Data Access Control in Cloud Computing," Int. J.Advanced Networking and Applications Volume: 01 Issue: 01 Page: (2011).

[6] G.Ateniese, K.Fu, M.Green, and S.Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005.

[7] W.Stallings, "Cryptography and network security," LPE Forth Edition, ISBN-978- 81-7758-774-6.

[8] S.D.C. di Vimercati, S. Foresti, S.Jajodia, S.Paraboschi, and P. Samarati, "Over encryption: Management of access control evolution on outsourced data," in Proc. Of VLDB'07, 2007.

[9] H.Zhong, and H.Zhen, "An Efficient Authenticated Group Key Agreement Protocol," Security Technology, 2007 41st Annual IEEE International Carnahan Conference on, vol., no., pp.250-254, 8-11 Oct.2007.

[10] S. K. Harit, S. K. Saini, N. Tyagi, and K. K. Mishra, "RSA Threshold Signature Based Node Eviction in Vehicular Ad Hoc Network," Information Technology Journal, 2012, ISSN 1812-5638, in Asian Network for Scientific Information.