International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

A Survey Paper on Data Security in Cloud Computing using Threshold Cryptography and User Revocation

Nikeetaa P. Choudharri[1], Prof. Shripadrao Biradar[2]

[1] M.E. II Computer, nikki231.nc@gmail.com, 9673931228

Abstract-Cloud computing is extremely well known in associations and foundations on the grounds that it gives stockpiling and computing administrations at low cost. Nonetheless, it additionally presents new difficulties for guaranteeing the confidentiality, integrity and access control of the information. Some methodologies are given to guarantee these security prerequisites however they are needed in a few routes, for example, infringement of information confidentiality because of plot assault and substantial calculation (because of substantial no keys). To address these issues we propose a plan that uses threshold cryptography in which information proprietor partitions clients in gatherings and gives single key to each client bunch for decoding of information and, every client in the gathering shares parts of the key. In this paper, we utilize ability rundown to control the access. This plan not just gives the solid information confidentiality additionally lessens the quantity of keys.

Keywords- Outsourced data, malicious outsiders, access control, authentication, capability list, threshold cryptography, user revocation.

INTRODUCTION:

Cloud computing is another and fast developing innovation in field of computation and storage of data. It gives storage and computing as a service at exceptionally attractive expense. It gives services according to three fundamental service models infrastructure as a service (IaaS), platform as a service (PaaS) 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 autonomous, rapid elasticity and measured scale service [1]. These characteristics make cloud significant. Commercial enterprises and establishments are misusing these characteristics of cloud computing and increasing their benefit and income. That is why, commercial enterprises are moving their organizations towards cloud computing. Notwithstanding, data security is a major obstacle in the way of cloud computing. Individuals are as yet fearing to abuse the cloud computing. A few individuals trust that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it. They are pretty much right[2][3]. Data of data proprietors are prepared and put away at external servers. Along these lines, confidentiality, integrity and access of data turn out to be more vulnerable. Since, external servers are operated by commercial service providers, data proprietor can't trust on them as they can utilize data for their advantages and can ruin organizations of data proprietor[4]. Data proprietor even can't trust on users as they may be malicious. Data confidentiality may violet through plot attack of malicious users and service providers.

To accomplish fine-grained information access control, the methodology has utilized capacity list [5]. It is fundamentally line based decay of access framework. In ability rundown approved information and operations for a client are indicated. It is preferable suit over Access Control List (ACL) [6][7][8] in light of the fact that ACL determines clients and their allowed operation for every information and record. It is essentially wasteful that two clients require same information and have same operations on it. In this paper, the methodology has utilized the altered Diffie-Hellman calculation to create one time shared session-key in the middle of CSP and client to secure the information from pariahs. To guarantee information honesty the methodology has utilized MD5 [4].

LITERATURE SURVEY

1) Attribute based Proxy Re-Encryption for Data Confidentiality in Cloud Computing Environments

AUTHORS: Jeong-Min Do

Key Policy-Attribute Based Encryption (KP-ABE) and Proxy Re-Encryption(PRE) are proposed to ensure data confidentiality and access control 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 problem, 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..

2) How to share a secret

AUTHORS: Adi Shamir

This paper proposes a schema which shows how to partition data into fragments in such way that it becomes 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 robust 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.

3) Secure Data Access in Cloud Computing.

AUTHORS: Sunil Sanka

Cloud computing is used by cloud users to outsource their sensitive and confidential data to cloud service providers 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 data security and access control problems but they increase the computational overhead on the data owner as well as the cloud service provider as they need to manage the keys as well as their distribution. In this paper, 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 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 provide authorized data access that will solve the problem of key management and its distribution at cloud service provider. The proposed approach is efficient and secure under existing security models.

4) Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage

AUTHORS: GIUSEPPE ATENIESE

Blaze, Bleumer, and Strauss (BBS) proposed an application, in 1998, known 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 rapid and efficient re-encryption will become tremendously popular as a solution for dealing with encrypted file systems. The technique known 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 a efficient way to provide security and also delivers the a way of providing access control to a file system security.

5) Capability-based Cryptographic Data Access Control in Cloud Computing

AUTHORS: Chittaranjan Hota

Cloud computing supports large data storage by using clusters of computers which has made it as a popular idea in computing world. It delivers the newest method for making computing resources work as a service. It describes not only a platform but also a type of application. It uses dynamic technique for configuring, allocating and de-allocating servers whenever they are needed. Cloud computing is used by cloud users to outsource their sensitive and confidential data to cloud service providers which leads to carry out research work on data security and access control of that data. There are many solutions that are available which make use of cryptographic techniques to solve these security and access control problems but they increase the overhead of the data owner as well as the cloud service provider as they need to manage the key as well as their distribution among the users. In this paper, 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 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 provide authorized data access that will solve the problem of key management and its distribution at cloud service provider. The proposed approach is efficient and secure under existing security models.

EXISTING SYSTEM:

The existing scheme uses threshold cryptography in which data owner divides users in groups and gives single key to each user group for decryption of data and, each user in the group shares parts of the key. In this paper, they use capability list to control the access. This scheme not only provides the strong data confidentiality but also reduces the number of keys.

PROPOSED SYSTEM:

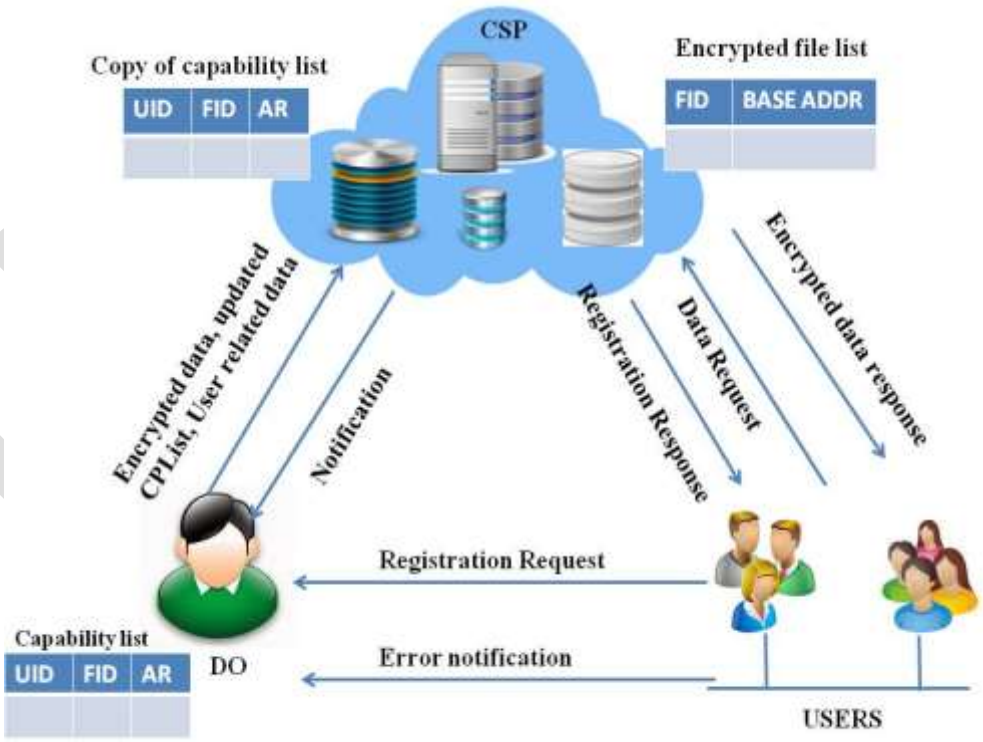
1. **User Revocation:**

   User revocation is the main challenge in previous scheme then we consider forward secrecy & backward secrecy. Forward secrecy is redefined in secure cloud sharing, which means that newly joining group members can decrypt and read all the shared files now and before. When a member leaves the group, he/ she will lose the ability to download and read the shared data ever again, which is called backward secrecy in cloud based group sharing.

2. **Data Dynamic Operation:**

   Data dynamics are most general forms of data operation, such as block modification, insertion, and deletion.

SYSTEM ARCHITECTURE:



CONCLUSION and FUTURE SCOPE:

We introduced another methodology which gives security for information outsourced at CSP. Some methodologies are given to secure outsourced information yet they are experiencing having huge number of keys and intrigue assault. By utilizing the threshold cryptography at the client side, we shield outsourced information from agreement assault. Since, DO stores its information at CSP in scrambled frame and, keys are known just to DO and regarded clients bunch, information confidentiality is guaranteed. To guarantee fine-grained access control of outsourced information, the plan has utilized ability list. Open key cryptography and MD5 guarantee the element verification and information integrity individually. Open key cryptography and D-H trade shielded the information from untouchables in our methodology. No of keys (on the grounds that in threshold cryptography, there is a single key comparing to every gathering) have decreased in the proposed plan.

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 FirstACIS/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-13:978-0-07-068351-8.

[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, 2007.207

[9] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats, "*Threshold Cryptography Based Data Security in Cloud Computing*", 2015 IEEE International Conference on Computational Intelligence & Communication Technology.

[10] R. S. Fabry, "*Capability-Based Addressing*," in Communications of the ACM, 17(7), July 1974, pp. 403-412.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-based encryption for fine-grained access control of encrypted data*," Association for Computing Machinery, in Proc. of CCS'06, 2006.

[12] N. Bennani, E. Damiani, and S. Cimato, "*Toward Cloud-Based Key Management for Outsourced Databases*," Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual, vol., no., pp.232-236, 19-23 July 2010.

[13] A. Shamir, "*How to share a secret*," Communications of the ACM, v.22 n.11, p.612-613, Nov. 1979. [Online].

Available:http://portal.acm.org/citation.cfm?id=359168.359176.