ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

REVIEW ON SECURITY ENHANCEMENT FOR CLOUD DATA STORAGE USING THRESHOLD CRYPTOGRAPHY

Miss J.J.Ghule,Miss J.R.Khebade,Miss S.A.Landage
Department of Computer Engineering,JCEI's Jaihind College Of Engineering,Kuran,India.

ABSTRACT

In organizations and institutions Cloud computing is very popular because it provides storage and computing services at very low cost. However, for ensuring the confidentiality, integrity and access control of the data it also introduces new challenges. Some approaches are given to ensure these security requirements but they are lacked in some ways such as destruction of data confidentiality due to collusion attack and heavy computation (due to large no keys). We propose a scheme that uses threshold cryptography To address these issues in which data owner divides users in groups and gives single key to every user group for decryption of data and, each user in the group shares parts of the key. In this paper, to control the access we use capability list. This scheme provides the strong data confidentiality as well as reduces the number of keys.

KEYWORDS: Outsourced data, Malicious outsiders, Access control, Authentication, Capability list, Threshold Cryptography.

INTRODUCTION

In field of computation and storage of data Cloud computing is a new and fast growing technology. At very attractive cost It provides storage and computing as a service. It provides 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 independent, rapid elasticity and measured scale service. These characteristics make cloud significant. Industries and institutions are exploiting these characteristics of cloud computing and increasing their profit and revenue [1]. That is why, industries are shifting their businesses towards cloud computing.

However, in the way of cloud computing data security is a major obstacle. To exploit the cloud computing People are still fearing. Some people believe that cloud is unsafe place and once you send your data to the cloud, you lose complete control over it [8][9]. 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 spoil 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 given 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 issues we propose a scheme. In this scheme, there are basically three entities: Data Owner (DO), Cloud Service Provider (CSP) and Users. Users are divided in groups on some basis such as location, project 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 number of users will present. This scheme not only provides data confidentiality by all means but also reduces the number of keys. To achieve fine-grained data access control, the approach has used capability list [6]. It is basically row-based decomposition of access matrix. In capability list authorized data and operations for a user are specified. It is better suit than Access Control List (ACL) [5][10][16] because ACL specifies users and their permitted operation for each data and file. It is practically inefficient that two 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 CSP and user to protect the data from outsiders. To ensure data integrity the approach has used MD5 [4].

RELATED WORKS

Data confidentiality and access control 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 (DO, CSP, 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 additional 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 [13] is the group-key scheme. In group-key scheme, there is a single key corresponding to each 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 CSP and a user 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 data confidentiality and access control. 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 can't see data stored at it as data are encrypted. Data are further encrypted by one time secrete session-key shared between CSP and user by the modified Diffie-Hellman protocol to protect 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 each 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 team and group 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 software and hardware industries, institutes, banks and medicals fields. There is provision of hierarchy of access in this scheme which makes this scheme more useful and realistic. For Example, an university has vice-chancellor, hods, teachers, clerklier-staff and students. Each one has different level of access right.

MODEL AND ASSUMPTIOMS

Previously in the existing system,we suppose that our model is composed of three entities: a CSP, a DO and many users associated with DO.CSP is the cloud service provider which stores large amount of data on the cloud.DO can upload,download and update its data on CSP securely in encrepted format.DU are the data users and they are unauthonticate persons ,thus they cannot directly acees the data of DO from the CSP.Initially, all users are registered at DO. During registration users send their credentials to DO. We assume that user's credentials are sent securely to DO. A user can get data from CSP in a confidential manner after successful authentication of himself at CSP. We assume that CSP has a large capacity and computational power. We also assume that no one can breach the security of CSP. Further we assume that the algorithm which is used to generate the secrete keys for encryption, is secure at DO.

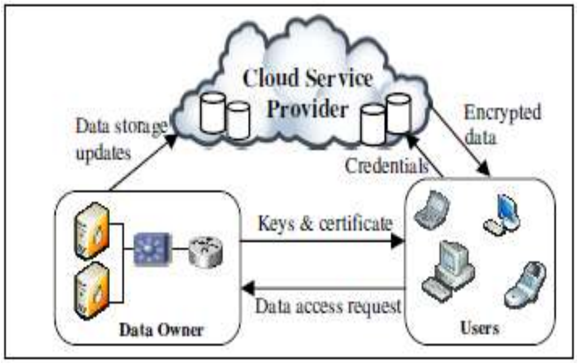

Fig. 1. Architecture of the Exesting System.

DO has storage capacity to store some files and data and, he can execute programs also at CSP to manage his files and data.For first time request from user DO provides the secure key and certificate to user.

User can use this key to acces the data from CSP.If the same user wants to access the same file o next times.For the convenience of user Do must be stayed online continuously. If the same user wants to access the same file o next times ,and if DO is offline then users must have to wait for DO to come online and then user can able to perform its further activity with Do.But for Do it is not possible to stay continiously online.This is the main drawback of this existing system and it is overcome in next proposed system.

PROPOSED SYSTEM

There are some drawbacks of the existing system.These drawbacks are overcome in the proposed system by using the concept of CPList and Threshold cryptography.

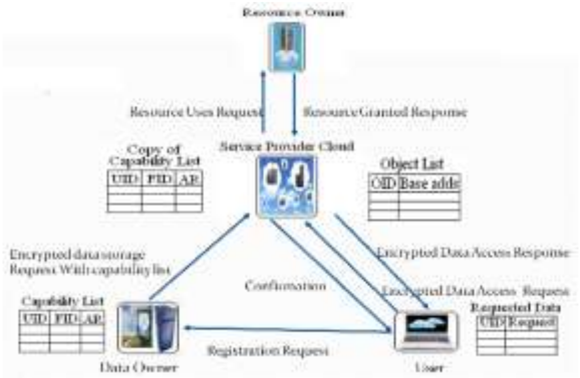

Fig. 2. Communication Model in the Proposed Scheme

For single userWe are using modified Diffie-Hellman and public key 203 cryptography to secure communication between CSP and user. Modified Diffie-Hellman protocol is used to create one time session-key between CSP and user. Fig.2. illustrates the secure communication between entities in the proposed scheme.For secure communication between different entities and secure access to data we present a complete model. There are four algorithms in the proposed scheme. Algorithm 1 describes secure communication of data between DO and CSP moreover this algorithm insures data confidentiality and, authentication of DO and CSP. Algorithm 2 describes procedures which DO and CSP apply after a new file creation in respect. Algorithm 3 describes about secure communication of data between CSP and user. In this algorithm user's authorization is also checked. Algorithm 4 describes the threshold cryptography technique for decryption of a user's file. Algorithm 4 is applied at user side where number of keys is reduced (one key corresponding to one group) and no threat of collusion attack as in group-key scheme. To understand proposed scheme better we take an example of real life scenario, DO may be a software industry who stores its data on to the CSP and the users may be its employees who view their data from the CSP. DO divides users in groups on some basis such as project basis and encrypts the data of each group with a single symmetric key (KT) and, it gives parts of the symmetric key (KT) to each user of the group. DO computes digest of data by using 128-bit MD5 hash algorithm and then encapsulates the digest and data using the symmetric key (KT).

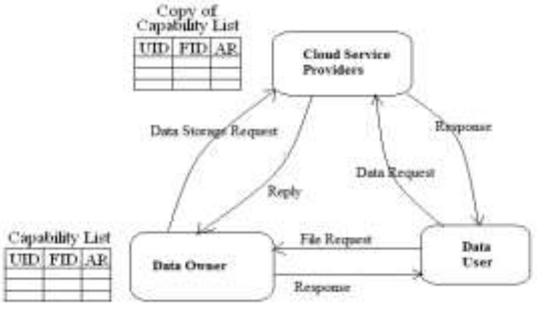

Fig.2. Block diagram of the Proposed Scheme.

This in turn, provides strong data confidentiality and integrity. DO then fills the entries such as UID, FID and AR in Capability List corresponding to each new user. DO then encrypts Capability List and encapsulated things with its private key after that public key of CSP and, then sends all things to CSP. These encryptions ensure confidentiality and authentication between DO and CSP.

CONCLUSION

In this paper, a new approach present here which provides security for data outsourced at CSP. To secure outsourced data some approaches are given but they are suffering from having large number of keys and collusion attack. By employing the threshold cryptography at the user side, we protect outsourced data from collusion attack. Since, DO stores its data at CSP 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.

ACKNOWLEDGEMENTS

We would like to take this opportunity to express our profound gratitude and deep regard to my Project Guide, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

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 206 ACIS/JNU International Conference on, vol., no., pp.248-251, 23-25 May 2011.

[2] 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.

[3] 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.

[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] 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.

[6] 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).

[7] 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.

[8] T. Mather, S. Kumaraswamy, and S. Latif, “Cloud Security and Privacy," O'Reilly

[9] Media, Sep. 2009.

[10] 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.

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

[12] G. Miklau, and D. Suciu, “Controlling access to published data using cryptography," in Proc. of 29th VLDB, Germany, Sept 2003.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in Proc. of IEEE INFOCOM 2010, 2010.

[14] 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.

[15] 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.

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

[17] 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.