An Automated SAN Solutions Overcome by Threshold Cryptography for Security by using Cloud Computing

Priyanka Khandekar[1] Kishor Kolhe[2]
[1,2]Department of Information Technology
[1,2]MIT college of engineering, Pune University, India

Abstract— Fast growth of data intensive applications has caused a changed in the traditional storage model. The server to disk approach is being replaced by storage area network (SANs), which enable storage to be externalized from server, thus allowing storage devices to be shared among multiple server by using threshold cryptography to secure data. A storage area network is a secure high speed data transfer network that provides access to consolidated block level storage to resolve this issues we have proposed a scheme named threshold cryptography within which information from owner will be divided among its users in cluster and partial key will be shared with all user for decryption.it has an virtual process to extend the storage capacity without any HDD attached to the client host server. SAN devices appear to server as attached drives, eliminating traditional network bottle neck. The partial key will be used by the user for decryption. However, it also introduce new challenges for ensuring the confidentiality, integrity and access control of data so to provide data security, data integrity threshold cryptography technique is used. The proposed scheme uses capability list to control the access. This proposed scheme not only pro-videos the study information con denasality however additionally reduces the quantity of keys.

Key words: Encryption, SANs, Outsourced data, access control, threshold cryptography

I. INTRODUCTION

Cloud computing is very popular in organizations and institutions because it provide storage and computing services at very low cost. However, it also introduces new challenges for ensuring the confidentiality, integrity and access control of the data. some approaches are given to ensure these security requirement but they are given to ensure these security requirement but they are lacked in some ways such as violation of data confidentiality due to collusion attack and heavy compution.To address these issues we propose a scheme that uses threshold cryptography in which data owner divides users in group 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, we use capability list to control the access. This scheme not only provide the strong data confidentiality but also reduce the number of keys. 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]. 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].by using AES ,RSA1,RSA2 algorithms to generate one time shared key session with highly security as it has three times encryptions.

II. RELATED WORK

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 its 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. Communication model of the proposed scheme somehow matches with it [4] but proposed scheme is more secure and reduces number of keys. 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.

III. PROPOSED ALGORITHM

A complete model for secure communication between different entities and secure access to data. 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 thegroup 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.

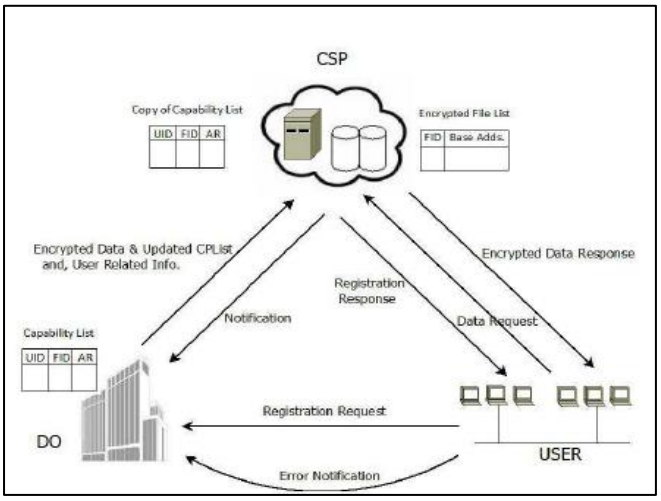


Fig. 1: Communication model in proposed system

Our model is composed of three entities: a CSP, a DO and many users associated with DO. 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. DO then divides users in groups and provides encryption keys, tokens, algorithm (MD5) and other necessary things for secure communication to user groups in response of registration. 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. DO

We present a complete model for secure communication between different entities and secure access to data. There are three 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 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 AES hash algorithm and then encapsulates the digest and data using the symmetric key (KT). 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.

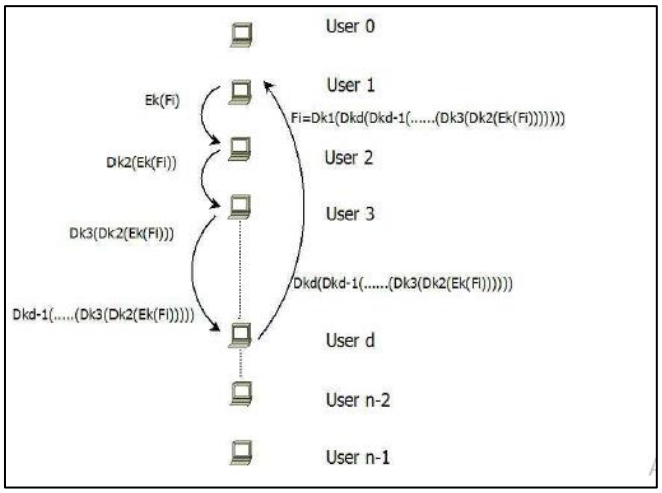


Fig. 2: Process of decryption

A. Algorithm 1: Procedure to be followed by CSP after getting encrypted File and Capability List from DO

It describes the process what CSP do after getting encrypted data and Capability List from the DO. CSP decrypts the message using its own private key and the public key of data owner and stores the encrypted data and Capability List in its storage. CSP then updates the encrypted File List and Capability List. Since, data are encrypted using symmetric key (KT) which is known only to DO and respected user group, CSP can't see data even though user's credential comes through it.

B. Algorithm 2: Procedure to be followed after a new File creation

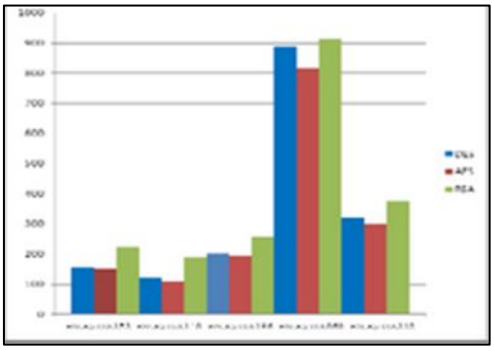
The procedure required after a new File creation. When a new File is created, DO fills entries for that File in Capability List containing UID, FID and AR. DO generates a symmetric key (KT) and encrypts File with that symmetric key (KT). Now, DO encrypts the updated CPList, Encrypted File and symmetric key (KT) with its private key after that public key of CSP and sends these to the CSP. When CSP receives these, it updates Capability List, Encrypted File List and sends encrypted symmetric key (KT) to respective user group. Users of the user group then decrypt the message and get their own parts of the symmetric key (KT). To avoid man-in-middle and replay attack we use nonce and timestamp in each message. After getting the details, user can request to CSP for data.

C. Algorithm 3 Algorithm for Decryption of a File for User 1

which resembles the threshold cryptography technique [2][14], describes the procedure how a File is decrypting for User 1. After getting encrypted message, user's main concern how to decrypt it because he alone can't decrypt. So, he first updates PKS Vector (Initially, all bits of it are zero) with his key component and then sends PKS Vector and encrypted message to next user of same group. The next user then decrypts the message and updates the PKS Vector with his key component. This is continuing until all bits of PKS Vector are one. Here, we can see that application is not

using all key components (Only threshold no of key components). After this, data are sent back to initiator user. Initiator user then decrypts the message and gets it. Initially, User 1does not decrypt message (M), he just updates the PKS Vector.

IV. RESULTS



Graph 1: showing the time consumption on processing

Here it is used for saving cost of company also due to three algorithms it has three times encryptions ,it reduces multiple keys .

V. CONCLUSION & FUTURE WORK

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 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. It reduces multiple keys because of algorithms which are used, as its three times encrypted it maintain security. Also new user and group is updated.

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, 23-25May 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] A. 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] 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 Media, Sep. 2009.

