ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

EFFECTIVE ACCESS CONTROL FOR DYNAMIC USERS IN CLOUD GROUPS

[1]D.Sterlin Rani, [2]U.Lavanya, [3]J.Jenefar, [4]M.Devika
[1]Assistant Professor, Dept of CSE ,Kings Engineering College,
[2,3,4]U.G Students, Dept of CSE, Kings Engineering College.

Abstract-In cloud computing, users can share data among group members with the characters of less maintenance and little management cost. Sharing data must have security guarantees, if they are out sourced. Sharing data while providing privacy preserving is still a challenging problem, when change of the membership. It might cause to the collusion attack for an unsecured cloud. For existing technique, security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. We propose a secure data sharing scheme for dynamic users. Key distribution done without any secure communication channels and the user can get the individual key from group manager. To prevent the unauthorized use of data accessing and create duplicate data on cloud the encryption technique to encrypt the data before stored on cloud server. Dropbox is proposed for cloud storage. All files of data owners are encrypted using AES algorithm and stored in real cloud. A secure architecture for handling file access in a dynamic cloud group. The user belonging to a particular group is analysed and identified. After that a private key is sent to the user by the group manager in the encrypted format using RC4 encryption algorithm.

Key words- Authority user verification, Security, File access, Collusion attack.

INTRODUCTION

Cloud Computing is an innovative technology that is revolutionizing the way we do computing [1]. The key concept of cloud computing is that you don't buy the hardware, or even the software, rather you rent some computational power, storage, databases, and any other resource, making your investment smaller and oriented to operations rather than to assets acquisition. In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive.

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better resource utilization. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data [1]. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers.

However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud.

Hybrid services like Box, Dropbox work in the cloud because they store a synced version of your files online, but they also sync those files with local storage. Synchronization is a cornerstone of the cloud computing experience, even if you do access the file locally. Dropbox is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration.

The Dropbox application is available for Windows, Macintosh and Linux desktop operating systems. There are also apps for iPhone, iPad, Android, and BlackBerry devices. The service provides 2 gigabytes (GB) of storage for free and up to 100 GB on various for-fee plans. Another option, Dropbox for Teams, provides 350 GB storage. The user data is stored on Amazon's

Simple Storage Service (S3) and protected with Secure Sockets Layer (SSL) and Advanced Encryption System (AES) 128-bit encryption.

SSL (Secure Socket Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This secure link ensures that all data transferred remains private. It's also called TLS (Transport Layer Security). Millions of websites use SSL encryption everyday to secure connections and keep their customer's data safe from monitoring and tampering.

AES algorithm is used to store those encrypted strings and later on want to decrypt it while retrieving the data. Many people face problem while decrypting the encrypted data as the KEY used for encryption if stored as String in database. For encryption we must use a secret key along with an algorithm.Group manager makes sure that the revoked users access the file if they conspire with untrusted cloud duplicate check. As we use the Secure protocol for anti-collusion attack there is faster recovery and processing of data. This would significantly decrease the processing time of load balancer and provides Effective and Efficient usage of cloud Storage Space.

PREVIOUS WORKS

Kallahalla et al. [3] presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. However, the file-block keys need to be updated and distributed for a user revocation. Therefore, the system had a heavy key distribution overhead. Other schemes for data sharing on untrusted servers have been proposed in [4], [5]. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

Yu et al. exploited and combined techniques of key policy attribute-based encryption [7], proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. However, the single- owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

Lu et al. [8] proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute based encryption techniques [9]. Each user obtains two keys after the registration while the attribute key is used to decrypt the data which is encrypted by the attribute-based encryption and the group signature key is used for privacy preserving and traceability. However, the revocation is not supported in this scheme. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cumulus cloud, accepting connections and doling out information as it floats.

EXISTING SYSTEM

In existence private key distribution is based on the secure communication channel. Secure communication means the text functions as a fully encrypted peer to peer text communication between any two people in a private group. In ABE, a message is encrypted for a specific receiver using the receiver's public key. In this case, which user have private key can share data unfortunately revoked user also can share data. Revoked user means who have changed their membership. Therefore, secure communication channel is a strong assumption but difficult to use. Existing cloud storage applications doesn't give complete data security. Extra storage consumption resulting in the extra storage cost for data application in the cloud. Cloud storage is not efficiently utilized. Replica of data is possible.

ABE(ATTRIBUTE BASED ENCRYPTION)

Attribute Based Encryption is a public key cryptography. A message is encrypted for a specific receiver using the receiver's public key. ABE goes one step further and defines the identity not automatic but as a set of attributes, e.g. roles and messages can be encrypted with respect to subsets of attributes or policies defined over a set of attributes. The key issue is, that someone should only be able to decrypt a cipher text if the person hold a key for "matching attributes" where user keys are always issued by some trusted party. ABE Algorithm suffers mainly from two drawbacks: non-efficiency and non-existence of attribute revocation mechanism.

DIFFIE-HELLMANN

Diffie-Hellmann key exchange is a secure method for exchanging cryptographic keys. An important problem in cryptography is how to establish keys for cryptographic protocols such as AES or DES, especially when the two parties are widely separated. Diffie-Hellmann algorithm depends on the difficulty of computing discrete logarithms. Fix a prime p, let α, β be nonzero integers mod p and suppose **$\beta\equiv \alpha^{x}$ (mod p).** The exponent x is referred as discrete logarithm of with respect to α. The problem of finding x is called discrete logarithm problem. There are two problems associated with diffie-hellmann key exchange

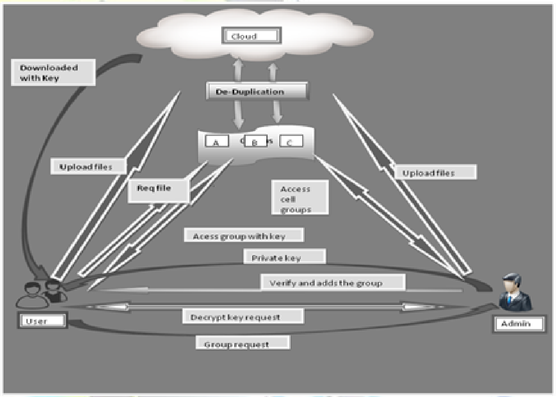
1.Computational Diffie-Hellmann Problem
2.Decision Diffie-Hellmann Problem

PROPOSED SYSTEM

The users can securely obtain their private keys from group manager. User send request to group manager for access the wanted group, at that time our system provide individual secure key to user without activation. Then group manager see the requests and activate the keys after confirm them. After user's private key gets activation, then only user can access the group. Our scheme has fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Access control is a trusted system. It prevents the unauthorized use of a resource.

Access control is the ability to limit and control to host systems and applications via communications links. In our proposed system the group manager performs the tasks such as, when an new user joins the group or a user has left the particular group, Update the whole user name list. Generate a secure key and encrypt the key without activation and send to the updated user list. Update the rights in the cloud server. We proposed public cloud named Dropbox for data storage. It can use completely free. When you register for dropbox account, you will automatically get 2 gigabytes of storage space. The space can be increased without paying a single cent. Group manager makes sure that the revoked users cannot access the file if they conspire with untrusted cloud. All files of data owners are encrypted using AES algorithm and stored in real cloud. We store the file data using 128 bit AES encryption and use an SSL securely transfer file between manager and members.

SYSTEM DESCRIPTION



In our proposed system, we propose a secure architecture for handling file access in a dynamic cloud group. The user belonging to a particular group is analysed and identified. After that a private key is sent to the user by the group manager in a encrypted format using RC4 encryption algorithm. The group manager performs the below tasks when a new user joins the group or a user has left the particular group, Update the whole user name list. Generate a secure key and encrypt the key without activation and send to the updated user list. Update the rights in the cloud server.

Data de-duplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, de-duplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. De-duplication can take place at either the file level or the block level. For file level de-duplication, it eliminates duplicate copies of the same file. De-duplication can also take place at the block level, which eliminates duplicate blocks of data that occur in non-identical files.

AES ALGORITHM

AES comprises three block ciphers, AES-128, AES-192, AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192, 256 bits respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. To using 128 bits AES algorithm because logically is an unbreakable.

STEPS:

1.Derive the set of round keys from the cipher key.
2.Initialize the state array with the block data(plaintext).
3.Add the initial round key to the starting state array
4.Perform nine rounds of state manipulation.

SSL(SECURE SOCKET LAYER)

SSL provides security service between TCP and applications that use TCP.SSL provides confidentiality using symmetric encryption and message integrity using a message authentication code. SSL is a computer networking protocol for securing connections between network application clients and servers over an insecure network, such as an internet. SSL runs above the transport layer and the network layer, which are responsible for the transport of data between processes and the routing of network traffic over a network between client and server, respectively, and below application layer protocols such as HTTP and the SMTP. [6] discussed about a method, End-to-end inference to diagnose and repair the data-forwarding failures, our optimization goal to minimize the faults at minimum expected cost of correcting all faulty nodes that cannot properly deliver data. First checking the nodes that has the least checking cost does not minimize the expected costin fault localization. We construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. We proposes efficient inferring approach to the node to be checked in large-scale networks.

RC4 ALGORITHM

RC4 encryption algorithm is a shared key stream cipher algorithm requiring a secure exchange of a shared key. It is used in the SSL/TLS (Secure Socket Layer/Transport Layer Security) standards that can be defined for communication between web browsers and servers. The symmetric key algorithm is used identically for encryption and decryption such that the data stream is simply XORed with the generated key sequence. It is one of the most widely software stream cipher and used in popular protocols, such as SSL (protect internet traffic).It's considered to be fast and simple in terms of software.

MODULES:

AUTHORITY USER VERIFICATION

At first Initial stage all users must create own username and password. After the Registration the user can login to their own space. This application verify the username and password which is either matched or not with the user registration form which is already created by the user while user registration process. If the valid user did not remember the username or password correctly the user can generate own password by using this application.

PRIVACY PRESERVING

In the Privacy preservation environments, a reasonable security protocol would be developed to achieve the following requirements.

AUTHENTICATION

A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

DATA ANONYMITY:

Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

USER PRIVACY

Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

FORWARD SECURITY:

Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

KEY DISTRIBUTION AND ACCESS CONTROL

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation. Once the user is revoked, the group manager creates the new encryption key for the specific group and transmits in an encrypted format using RC4 algorithm. Second the group manger updates the whole data list in the cloud server. Third the group manages updates the user list and activates the key for access.

DE-DUPLICATION

Data de-duplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, de-duplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. De-duplication can take place at either the file level or the block level. For file level de-duplication, it eliminates duplicate copies of the same file. De-duplication can also take place at the block level, which eliminates duplicate blocks of data that occur in non-identical files.

COLLUSION ATTACK

The user leaving a group termed as revoked users. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Thus our proposed system detects the revoked users and protects the data confidentiality and privacy.

SECURE DATA SHARING

Secure data sharing is performed using private keys generated and transmitted using secure communication channels. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels using RC4 algorithm.

CLOUD STORAGE

The group user can upload the files in real cloud server named dropbox. Duplication of files are checked and the files is been uploaded in the cloud server. To get a file, the user needs to send a request to the cloud server. The cloud server will also check the user's identity before issuing the corresponding file to the user. During file access the user key has to matched by the group manager and the requested file can be downloaded by the group users.

CONCLUSION

In this paper, we propose a secure data sharing scheme for dynamic members. The admin are having the authority to transfer the file between admin and group members. Admin has the private key will be known to the user and file will be transferred securely using access control.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,“A view of cloud computing,” Commun. ACM, vol. 53, no. 4,pp. 50–58, Apr. 2010.
[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.
[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Plutus: Scalable secure file sharing on untrusted storage,”in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.
[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing remote untrusted storage,” in Proc. Netw. Distrib. Syst. SecuritySymp., 2003, pp. 131–145.
[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proc. Netw. Distrib. Syst. Security Symp., 2005,pp. 29–43.
[6] Christo Ananth, Mary Varsha Peter, Priya.M., Rajalakshmi.R., Muthu Bharathi.R., Pramila.E., “Network Fault Correction in Overlay Network through Optimality”, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Volume 2, Issue 8, August 2015, pp: 19-22
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,”in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.
[8] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure provenance: Theessential of bread and butter of data forensics in cloud computing,” in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.
9.B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography,2008,pp.53–70.