International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
SharadchandraPawar college of Engineering, Dumbarwadi, Pune 410504, Organizes
National Conference "MOMENTUM-17", 14th & 15th February 2017
Available online at www.ijrat.org

An Efficient And Secure Data Sharing By Preventing Collusion Attack In Cloud

Jyoti Pingat[1], Swati Mandwade[2],
1Student, Savy Software Pvt.Ltd,Pune
2 Student, ,Savy Software Pvt.Ltd,Pune
Email: jyotipingat123@gmail.com[1],swatinmandwade19@gmail.com[2]

Abstract-Today data sharing and maintaining its security is major challenge. User in the data sharing system upload their file with the encryption using private key. This property is especially important to any large scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this paper provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. SHA algorithm is used by the trusted authority to generate the key and that key will get share to user as well as the owner. The trusted authority module receives encrypted file using AES Algorithm from the data owner and computes hash value using MD-5 algorithm. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). Trusted authority send file to CSP module to store on cloud.

Index Terms-Security; Trusted Authority; Advanced Encryption Standard (AES); Cloud Service Provider (CSP).

1. INTRODUCTION

Cloud computing is the biggest buzz in computer world now a days. Cloud computing is an internet based modern technique, which is capable of providing us various resources. It is providing excellent facilities by flexible infrastructure. Cloud computing is based on client-server architecture. Cloud computing is a hub of various server and many database to store data. The availability of these resources are very flexible in nature i.e. few are available to customers free of cost but some on a pay as use basis. Along with this the customer is also allowed to access information and can utilize computer resources from anywhere if having the internet access. Various security issues, like hacking, stealing, unauthorized access etc. are also emerging along with the emergence of the same [1]. These security related issues degrade the popularity of cloud computing. To overcome these issues we proposed a system, which can achieve secure key distribution and data sharing for dynamic group.

In cloud computing, cloud administration suppliers offer a deliberation of limitless storage room for customers to host information [4]. Cloud computing, with the attributes of characteristic information sharing and low support, gives a superior usage of assets. It can help customers diminish their money related overhead of information administrations by moving the neighborhood administrations framework into cloud servers.

To safeguard information protection, a typical methodology is to encode information records before the customers transfer the scrambled information into the cloud [5]. Be that as it may, security concerns turn into the principle imperative as we now outsource the capacity of information, which is conceivably touchy, to cloud suppliers. Lamentably, it is hard to plan a protected and effective information sharing.

The rest of the paper has been organized as: section 2 highlights the related work along with their downsides, section 3 discusses the proposed work of system. section 4 followed by conclusion and references.

2. RELATED WORK

Kallahalla et al 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. Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

The author Kallahalla et al. exhibited a cryptographic storage framework that empowers secure information sharing on conniving servers in light of the methods that isolating documents into record bunches and encoding every document bunch with a document square key. Not with standing, the document square keys should be redesigned and conveyed for a client denial; accordingly, the framework had a substantial key circulation overhead. Different plans for information sharing on untrusted servers have been proposed. In any case, the complexities of client support and repudiation in these plans are straightly expanding with the quantity of information proprietors and the denied clients. Lu et al. proposed a secure provenance scheme by leveraging group signatures and cipher text-policy attribute based encryption techniques. 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.

Liu et al. introduced a protected multi-proprietor information sharing plan, named Mona. It is asserted that the plan can accomplish fine-grained access control and repudiated clients won't have the capacity to get to the sharing information again once they are revoked. Be that as it may, the plan will effortlessly experience the ill effects of the plot assault by the renounced client and the cloud [1]. The revoked client can utilize his private key to unscramble the scrambled information document and get the mystery information after his renouncement by contriving with the cloud. In the period of document access, most importantly, the denied client sends his solicitation to the cloud, then the cloud reacts the comparing encoded information record and revocation list to the renounced client without confirmations. Next, the denied client can figure the decoding key with the assistance of the assault calculation. At long last, this assault can prompt the repudiated clients getting the sharing information and uncovering different privileged insights of real individuals. Nabeel et al. proposed a protection safeguarding policy based content sharing plan in broad daylight mists. However, this plan is not secure in view of the frail insurance of responsibility in the period of character token issuance.

3. PROPOSED WORK

In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.

We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. We propose a secure data sharing scheme which can be protected from collusion attack. 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. Our scheme can achieve secure user revocation with the help of polynomial function.

Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme.

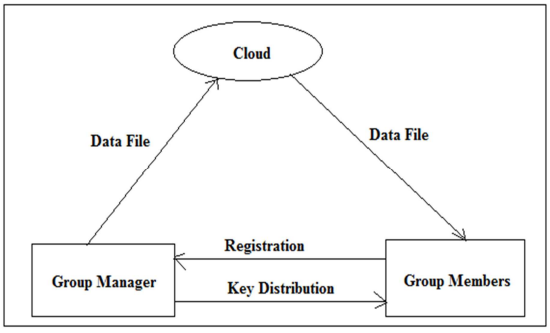

Fig. 1. System Architecture

We give security investigation to demonstrate the security of our plan. Furthermore, we additionally

perform reproductions to exhibit the productivity of our plan.

Data Owner: (Group Member)
In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Cloud Server:
The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Data Integrity:
Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Group Manager:
The Group Manager who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the cloud data.

Data Consumer: (End User / Group Member)
In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the GM authority and the Data users are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

4. PROPOSED ALGORITHM

Algorithm 1: AES Algorithm

Algorithm finds the Proxy Re-Encryption : A PRE scheme is represented as a tuple of (possibly probabilistic) polynomial time algorithms (KG; RG; E; R; D). (KG; E; D) are the standard key generation, encryption, and decryption algorithms.

AES encrypts messages through the following algorithm, which is divided into 3 steps:

1. Key Generation:

Step 1: Choose two distinct prime numbers p and q.

Step 2: Find n such that $n = pq$.
n will be used as the modulus for both the public and private keys.

Step 3: Find the totient of n, $\phi(n)$

$\phi(n)=(p-1)(q-1)$.

Step 4: Choose an e such that $1 < e < \phi(n)$, and such that e and $\phi(n)$ share no divisors other than 1 (e and $\phi(n)$ are relatively prime).

Step 5: Determine d (using modular arithmetic) which satisfies the congruence relation

$de = 1 \pmod{\phi(n)}$.

In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or $\phi(n)$.
This is often computed using the Extended Euclidean Algorithm, since e and $\phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e.
d is kept as the private key exponent.

The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption:

Step 1: Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.

Step 2: When Person B wishes to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.

Step 3: Person B computes, with Person A's public key information, the ciphertext c corresponding to

$c = me \pmod n$.

Step 4: Person B now sends message "M" in ciphertext, or c, to Person A.

3. Decryption:

Step 1: Person A recovers m from c by using his/her private key exponent, d, by the computation

$m = cd \pmod n$.

Step 2: Given m, Person A can recover the original message "M" by reversing the padding scheme.

This procedure works since,

$c = me \pmod n$,
$cd = (me)d \pmod n$,
$cd = mde \pmod n$.

By the symmetry property of mods we have that

$mde = mde \pmod n$.

Since $de = 1 + k\phi(n)$, we can write
$mde = m1 + k\phi(n) \pmod n$,
$mde = m(mk)\phi(n) \pmod n$,
$mde = m \pmod n$.

From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all m and the original message

$cd = m \pmod n$, is obtained.

5. CONCLUSION AND FUTURE WORK

System design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, 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. Future plan can accomplish secure client revocation, the revoked clients cannot have the capacity to get the first information documents once they are revoked regardless of the possibility that they scheme with the untrusted cloud. A future research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their data. Another research direction would be to give the data owner physical access control over the data. Instead of accountability, the data owner can create a set of access control rules on his data and send the data along with the access control policy. In this way, any member with access to the data can only use the data in such a way that abides by the access control policy. If a member attempts to make illegal copies of the data, the access control policy should "lock" the data to prevent the member from doing so.

Acknowledgments

I express my sincere thanks to my project guide Prof. G. S. Deokate who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of computer department for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a paper work.

REFERENCES

[1] Zhongma Zhu, Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, 2015.
[2] Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE has proposed a paper on "Public Auditing for Shared Data with Efficient User Revocation in the Cloud".
[3] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H Deng proposed a paper on "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.".
[4] Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student

Member, IEEE, and Elisa Bertino, Fellow, IEEE" proposed a paper on "An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds".

[5] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed paper on "Privacy Preserving Delegated Access Control in Public Clouds".

[6] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong" proposed a paper on "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing".

[7] KaipingXue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on "A Dynamic Secure Group Sharing Framework in Public Cloud Computing".

[8] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation".

[9] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification".

[10] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou" proposed a paper on "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing".

[11] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou" proposed a paper on "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security".