IMPLEMENTING DATA SECURITY USING ODD-EVEN THRESHOLD CRYPTOGRAPHY IN CLOUD COMPUTING

Deepali R. Kosare[1] , Devishree R. Naidu[2]
[1]M.Tech Student, [2]Assistant Professor,
Dept. of Computer Science &Engineering,
Shri Ramdeobaba College of Engineering And Management, Nagpur, India

Abstract

Cloud computing is undoubtedly beneficial for small and large scale enterprises because it provide services at very low cost. But there are certain issues and challenges faced by the user while using cloud computing with regard to security. However new challenges popped out to ensure confidentiality, integrity and access control of the data. In order to deal with this need for security, certain approaches are given but they failed to fulfil this requirement since there is violation of data confidentiality due to malicious insider, collusion attack and key management (due to heavy performance by using large no. of key). In order to tackle these issues we proposed odd-even threshold cryptography scheme in which data owner divides users in groups and further groups are divide into two user groups(i.e. odd and even user groups) and gives single key to each user groups for decryption of data. Distributed parallel processing is applied on two groups (i.e. odd and even user groups) for simultaneously performing two decryption processes. The main features of this scheme is that data are prohibiting from insider attack, also reduce the number of security key and it not only reduce decryption process time but also decrypts two file simultaneously.

Keywords: Cloud Computing, Threshold Cryptography, Malicious Insider, Collusion Attack, Odd-Even Threshold Cryptography.

I. INTRODUCTION

Cloud computing is a computing model, distributed on large scale in which small area of computing resources is available to users through the Internet and it also provides storage and computing services at a very low cost, so it has gain popularity in various organizations and institutions . The storage of terabyte data, generated by everyday is the biggest requirement of an IT industry. Thus, to meet this requirement it requires many of hardware, software and network infrastructures. Cloud computing solve this problem in cost effective manner. It has completely changed the structure not only IT Industry but some other sectors like education, healthcare sector. Cloud computing is growing very rapidly because of their features like resource capability, network infrastructure, storage capability, cost effective, quick access of information. The main characteristics of cloud computing are: Remotely hosted, ubiquitous, Resiliency, on-demand self service, rapid elasticity, broad network access, full managed by the provider. On other side all data is virtual and cloud is as open services and they make use of public network for their application and services, which are questionable regarding security issues. Data security is a prime obstacle in the way of cloud computing. People are still fearing to exploit the cloud computing. Some people believe that cloud is not a safe place and once you send your data to the cloud, you lose complete authority over it. They are more or less right. Data of data owners are taken care and stored at external servers. So, confidentiality, integrity and access of data become unprotected. Since, external servers are operated by commercial service providers, data owner can't trust on them as they can use data for their profits and can destroy businesses of data owner. Data owner even can't trust on users as they may be mischievous. Data confidentiality may violet through collusion attack of mischievous users and service providers. Some approaches are given to ensure these security requirements but

they are lacked in some ways such as violation of data confidentiality due to collusion attack and heavy computation (due to large no keys). To address these issues based paper propose a scheme that uses odd-even threshold cryptography scheme in which data owner divides users in groups and further groups are divide into two user groups(i.e. odd and even user groups) and gives single key to each user groups for decryption of data. Distributed parallel processing is applied on two groups (i.e. odd and even user groups) for simultaneously performing two decryption processes. This scheme not only provides the strong data confidentiality but also reduces the number of keys. 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 odd-even threshold cryptography technique. Such as software and hardware industries, institutes, banks, university and medicals fields.

II. LITERATURE SURVEY

Data confidentiality and access control are two major security requirements in cloud computing. Sometimes, more importance is given to security of data thus, forgetting the performance of system. For instance, we sometimes use to many keys for data security .As the keys are confidential there is a need to secure and maintain keys which itself is a additional work. Thus, it affects the performance of the system. So, reducing number of keys become more essential. This problem is solved by introducing scheme that provide not only data security but at the same time maintain the performance.An overall literature survey is presented here.

In 2007, HE Yong-Zhong (Assistant Professor) and HAN Zhen (Professor) Department of Computer Science and Engineering has published a research paper “An Efficient Authenticated Group Key Agreement Protocol”[2]. In this paper group-key agreement scheme is used. This scheme construct the session key by sharing equally contributed information from every group member and permit group members to agree on a session key to secure their communication. There is a single key similar 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 break whole data of the group to CSP. We know that CSP party is not trust worthy. It can make use of data owner’s data for its commercial profits.

In 2010 , S. Sanka, C. Hota(Dept. Of computer science,BIT institute-Pilani) and M. Rajarajan (Dept. Of IT, Northampton-London) has published a research paper “Secure Data Access In Cloud Computing“[4]. In this paper, symmetric key and capability list scheme 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. CSP is use as storage Medium for the encrypted data. Since, the stored data are encrypted, CSP is unable to see it. Data are further encrypted by one time secrete session-key shared between CSP and user by the Diffie-Hellman protocol to protect data from outsiders during the transmission between CSP and user. This scheme no doubt provides the 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 increases. These in turn increase the maintenance as well as security concern of key .So, as to secure the data we sometimes make use of so many keys. This extra work affect the system’s performance so, it is recommendable to reduce number of keys.

In 2015, S.K.Saroj, S.K.Chauhan, A.K.Sharma and S.Vats(CSE Department GCET, Greater Noida.) has published a research paper“Threshold Cryptography Based Data Security In Cloud Computing“[5]. in this paper i threshold cryptography scheme is used. In threshold cryptography, basically there are three entities: Data Owner, Cloud Service Provider and many users associated with Data Owner. 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. Parts of the key are distributed among the each user in the group. Data can be decrypted when at least threshold number of users will present. This scheme not only provides data confidentiality but also reduces the number of keys. This

scheme is best for preventing data security from collusion attack of malicious users and service providers and also maintains the system performance. But this technique takes more time for decryption process.

III. MODEL AND ASSUMPTIONS

To understand proposed scheme better we take model as an example of real life structure. In this model, there are three important entities: Data Owner, Cloud Services Provider and many Users. Data Owner may be a software industry who Store its data on to the CSP and the users may be its employees who view their data from the CSP. Initially, all users get them self registered at DO. During registration users send their information to DO. We imagine that user's information is sent securely to DO. DO then fills the entries such as UID, FID and AR in access right List corresponding to each new user. DO divides users in groups on some basis and further groups are divide into two user groups(i.e. odd and even user groups) and gives encryption keys(AES Algorithm),algorithm(MD5) and other required things for secure communication.

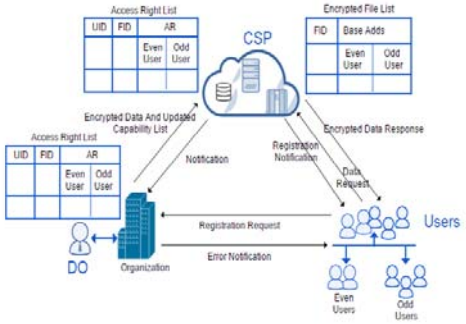

Fig. 1. Communication Model in the Proposed Scheme

This encrypted data are stored at CSP. These encryption algorithms ensure confidentiality and integrity between DO and CSP. User then request for data to CSP. CSP initiates modified D-H key exchanges with the user, if request is trustworthy. Modified Diffie-Hellman algorithms ensure confidentiality between CSP and users. Here user then decrypts the data by using Odd-Even Threshold Cryptography technique.

IV. PROPOSED SCHEME

Secret sharing scheme (n,n) refers to methods for distributing secret key amongst a group of users, each of whom is allocated a share of the secret key. The secret key can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. But this scheme take more time for reconstructing secret key when more number of users are present in one group.

Threshold cryptography *(t, n)* is the other type of secret sharing scheme there is one data owner and n users. The data owner gives a share of the secret key to the users, but only when specific conditions are fulfilled will the users be able to reconstruct the secret from their shares. The data owner accomplishes this by giving each user a share in such a way that any group of t (for threshold) or more users can together reconstruct the secret key but no group of fewer than *t* users can. Such a system is called a *(t, n)*-threshold scheme (sometimes it is written as an *(n, t)*-threshold scheme).But there are few challenges such as, if threshold value (t) is too small then there is possibility to attack on secret key and if threshold value (t) is too big then it take more time for reconstructing secret key. So, To address these above issues we propose a scheme that uses Odd-Even threshold cryptography(to/te,t) in which data owner divides users in groups and further groups are divide into two user groups(i.e. odd and even user groups) and gives single key to each user groups for decryption of data. Distributed parallel processing is applied on two groups (i.e. odd and even user groups) for simultaneously performing two decryption processes.

The figure below describes the decryption procedure, showing how a file is decrypted for User1 using Threshold Cryptography. After getting encrypted file ,user main concern is how to decrypt it because he alone can't decrypt .After getting encrypted message to user1, he just pass that message to the next user of the same group. After getting encrypted file user2 decrypt the same file using his own key and send it to the next user i.e. user3 and this process continue until the encrypted file reaches to the threshold user. Lastly, the encrypted file goes back to initiator user1 and user1 using his own key decrypt the encrypted file.

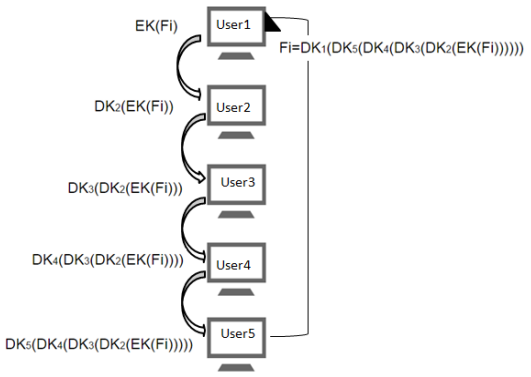

Fig. 2. Process of Decryption for User 1(t,n)

This scheme provides the strong data confidentiality and reduces the number of key. But this scheme take more time for decryption process and at a time only one file is decrypted. So, overcome this, we design odd-even threshold cryptography scheme. In this scheme we divide threshold users(t) into odd-even threshold user group(to/te,t).

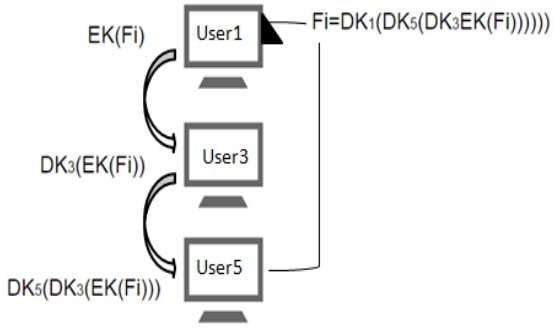

Fig.3 Odd Threshold Users Group (to,t)

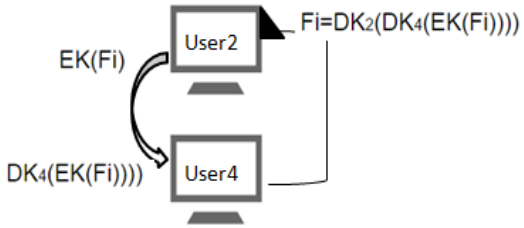

Fig.4 Even Threshold User Group (te,t)

This scheme not only provides strong data confidentiality but also reduce the decryption process time. It also reduces number of key. Here, we give access right to both odd and even users group for simultaneously performing decryption process.

V. CONCLUSION

In this paper, we introduced a new approach which provides

Security for data outsourced at CSP and reduces number of key. By employing the Odd-Even threshold cryptography at the user side, we protect outsourced data from collusion attack.

REFERENCES

[1] 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.

[2] 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.

[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] Sushil Kr Saroj, Sushil Kr Saroj, Aravendra Kr Sharma, and Sundaram Vats, ―Threshold Cryptography Based Data Security in Cloud Computing‖ IEEE International Conference on Computational Intelligence & Communication Technology,2015

[6] Kajal Chachapara and Sunny Bhadlawala, ―Secure sharing with cryptography in cloud computing‖ Nirma University International Conference on Engineering (NUiCONE), 2013

[7] Vikas Sagar and Krishan Kumar, ―Symmetric Key Cryptography Using Genetic Algorithm And BPNN ANN IEEE Encryption ―, 2015