International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 293 - 297

Data Security in Cloud Computing Using Threshold Cryptography and User Revocation

1.Nikeetaa P. Choudharri,
RMD Sinhgad School of Engineering,
Pune

2.Ms. Kanchan M. Varpe,
RMD Sinhgad School of Engineering,
Pune

Abstract—Cloud computing is extremely well known in associations and foundations on the grounds that it provides services at low cost. Nonetheless, it additionally presents new difficulties for guaranteeing the confidentiality, integrity and access control of the information. Few methodologies are proposed to guarantee these security prerequisites however they are needed in a few routes, for example, infringement of information confidentiality. To address these issues a plan is proposed that make use of threshold cryptography in which information proprietor partitions clients in gatherings and provides single key to each client bunch for decoding of information and, every client in the gathering shares parts of the key. This plan not just gives the solid information confidentiality additionally lessens the quantity of keys and manages access control and user revocation.

Index Terms—*Outsourced data, malicious outsiders, access control, authentication, capability list, threshold cryptography, user revocation.*

*****

1. INTRODUCTION

CLOUD computing is another and fast developing innovation in field of computation and storage of data. It gives storage and computing as a service at exceptionally attractive expense. It gives services as indicated by three essential service models infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).Storage as a service is fundamentally a platform as a ser- vice. The five characteristics of cloud computing are: on-interest service, self service, area self-ruling, quick flexibility and measured scale service [1]. These characteristics make cloud critical. Business ventures and foundations are abusing these characteristics of cloud computing and expanding their advantage and salary. That is why, commercial enterprises are moving their organizations towards cloud computing. In any case, data security is a noteworthy impediment in the method for cloud computing. Individuals are as yet fearing to abuse the cloud computing. A couple of people trust that cloud is perilous spot and once you send your data to the cloud, you lose complete control over it. They are pretty much right. Data of data proprietors are prepared and put away at external servers. Along these lines, confidentiality, integrity and access of data turn out to be more vulnerable. Since, external servers are worked by business service providers, data proprietor can't trust on them as they can use data for their favorable circumstances and can demolish associations of data proprietor [4]. Data proprietor even can't trust on users as they might be malicious. Data privacy might violet through plot assault of malicious users and service suppliers.

To accomplish fine-grained information ac- cess control, the methodology has utilized ca- pacity list [5]. It is fundamentally line based decay of access framework. In ability rundown approved information and operations for a client are indicated. It is preferable suit over Access Control List (ACL) [6][7][8] in light of the fact that ACL determines clients and their allowed operation for every information and record. It is basically inefficient that two clients require same information and have same operations on it. In this paper, the methodology has utilized the altered Diffie Hellman calculation to create one time shared session-key in the middle of CSP and client to secure the information from pariahs. To guarantee information honesty the methodology has utilized MD5 [4].

In this paper a study about the related work and its background is done in section 2, the proposed system is specified in section 3 which includes problem statement, objective and al- gorithms. System architecture is described in section 4. Section 5 includes discussion regarding implementation details which includes soft- ware specifications and mathematical model. Section 6 includes expected results and conclusion is specified in section 7.

2 RELATED WORK

Data confidentiality and access control are two essential requirements for providing security to the outsourced data in cloud computing. Many times, security of data considered first and performance of the system is neglected. Many schema make use of too many keys, as it is a way to provide security. But use of too many keys leads to additional work as these keys needs to be maintained. This additional work ultimately affects the performance of the system. So, it is desirable to reduce no of keys. So, a scheme is needed which must provides data security of outsourced data as well as maintain the performance. Many schemes are proposed to ensure these requirements.

The scheme proposed in [10] is the group key scheme. Group-key schema is a schema in which a single key is assigned to each group. All members of the group know the key and they can use that key for decryption process. Total numbers of keys are reduced as a single key is used instead of too many keys. But the

schema may lead to a problem known as collusion attack. Collusion attack between Cloud Service Provider (CSP) and users can leak the whole data of the group to the CSP if the group consists of single malicious user. CSP is an entity which is not trusted at all as it can use the data owner's data for its benefits.

The scheme proposed in [4] deals with data confidentiality and access control of the out- sourced data. In this scheme, encryption of data is done using the symmetric key shared between data owner and respective data users. CSP stores the data in encrypted format due to which it cannot use the data of its benefits. To protect the data from outsiders while trans- mitting the data between CSP and user data is again encrypted using one time secret session key known to the CSP and User. It makes use of modified Diffie Hellman protocol. This scheme provides data security but it has some drawbacks. Scheme uses a single key corresponding to each user and number of users can be large in number. So, large numbers of keys are needed in this scheme which ultimately increases the additional work related to the keys.

The scheme used in [8] makes use of access control list to provide access control of data. Access Control List is not an efficient approach as it specifies users and their allowed operation with respect to each file. Many applications make use of large number of files as well as they have large number of users. In such applications, ACL will require large amount of storage which will decrease the storage needed to store actual data.

3 PROPOSED SYSTEM

3.1 Problem Statement

The new difficulties for guaranteeing the con- fidentiality, integrity and access control of the data. Some methodologies are given to guarantee these security necessities however they are needed in a few courses, such as, infringement of data confidentiality because of collusion at- tack and overwhelming calculation (because of expansive no keys). This system give more security to the outsourced data in cloud computing. The system cope up with the collusion attack and decreases the computation as it uses less number of keys. The system efficiently manages the addition and deletion of the user in the group.

3.2 Objective

The objective of the system is to ensure the confidentiality, integrity and access control of the data as well as to solve the problem of user revocation in cloud computing environment.

3.3 Algorithm

In this section, a complete secure model used for communication between various entities and secure access to data is described. This paper defines the method used for secure trans- mission of data between Data Owner (DO) and CSP. This transmission also ensures data confidentiality and, authentication of DO and CSP.

When DO creates a new file some procedure is been followed by the DO and the CSP. Some procedure is applied to ensure secure trans- mission of data between CSP and user. Authorization of user is also done. An algorithm is proposed which makes use of threshold cryptography technique. Algorithm is applied by the user when it requests for a data file. This algorithm deals with less number of keys and also reduces the chances of collusion attack as it uses one key corresponding to one group. When CSP gets the encrypted data and the capability list from the data owner it decrypts that message using its private key followed by the public key of the data owner. Then it stores that encrypted data and capability list in its storage space. CSP then updates the encrypted File List and Capability List stored at its side. CSP cannot make use of data stored in its storage space because the data is in encrypted format. This data is encrypted using symmetric key (KT) which is shared by DO and corresponding data users.

DO follow some process when it creates a new data file. After creating a new file, DO makes entry of that file in the capability list which includes fields like, user identity (UID), file identity (FID) and access rights (AR). A symmetric key (KT) is generated by the DO which is used to encrypt that newly created file. DO also encrypts the updated capability list, encrypted file as well as the symmetric key (KT) by using its own private key first, followed by public key of CSP. Then it sends these encrypted data to CSP. When this en- crypted message is received by CSP, it makes entry in its capability list as well as encrypted file list and sends the encrypted symmetric key (KT) to corresponding data user group. When user receives this encrypted symmetric key he decrypts that message and get his own parts of the symmetric key (KT).

Modified Diffie Hellman algorithm is used for transmitting the data securely between CSP and user. Modified D-H algorithm is used to tackle the man-in-the-middle attack. When user has the keys and tokens it can request for that data from CSP. Modified D-H key exchange protocol is initiated by CSP, if request is from authentic user. Session Key (KS) is shared between CSP and the user by using modified Diffie Hellman algorithm. CSP encrypts the re- quested encrypted file and its message digest with the shared session key (KS) and sends it to the user. This double encryption ensures the confidentiality of data file between CSP and the user. User then decrypts the message by applying the algorithm described in next paragraph and calculates the message digest of the file received from CSP. If the generated message digest matches with the stored message digest then the received file is the original file, otherwise it is modified one. Error message is send to the CSP if the modified copy of file is received by the user.

Algorithm proposed in this scheme makes use of threshold cryptography technique. The algorithm describes the procedure how a File is decrypting for User 1. When user receives the encrypted file from CSP it needs to decrypt the file to get the data. Decryption of the

file cannot be done by using its own part of a key. Threshold number of users must provide their keys to decrypt the data. Decryption process makes use of Partial Key Set (PKS) vector. This PKS vector is initialized to zero at the beginning. User first updates the PKS vector with his part of key and then forwards the PKS vector and encrypted message to the next user in the same group. The next user follows the same process means updates the vector with his part of key and forwards it to the next user. This process is continued until all bits of vector are set to one. This ensures that system uses threshold number of key components instead of all key components. After receiving threshold number of key components, data is sent back to the user to request the data. Now, the data can be decrypted and can be used by the user.

Algorithm 1 Algorithm for Decryption of a File fo User 1

1: User 1 receives Encrypted File
$M \leftarrow Rece(Ek_{KT}(F\,i))$
2: Initially, all bits of PKS vector is zero. Here, PKS Vector indicates parts of the key. User 1 will update this PKS vector with the components he has
$PKS = PKS\ OR\ A_1$
3: User 1 forwards M and PKS to ith user of the group, who will decrypt it and update the PKS vector
$M = Dk_{KT_i}(M)$
$PKS = PKS\ OR\ A_i$
The ith user then forwards M and PKS to next user in the group. The next user performs same operation as ith user did. This process is continued.
4: if(PKS == 111111..... up to d bits) Go to step 5
Else
Go to step 3
5: Forward M to the user 1
User 1 then decrypts message (M) and get File
$F_i = Dk_{KT_i}(M)$

User revocation is the main challenge in previous scheme then we consider forward secrecy backward secrecy. Forward secrecy is redefined in secure cloud sharing, which means that newly joining group members can decrypt and read all the shared files now and before. When a member leaves the group, he or she will lose the ability to download and read the shared data ever again, which is called backward se- crecy in cloud based group sharing. Algorithms used for user revocation are as follows:

1) KeyGen(n): This randomized algorithm takes as input a parameter n, the number of individuals from the group. It outputs a group public keygpk, and also a new n- element vector of keys
gsk (gsk[1], gsk[2], ..., gsk[n]),
and an n-element vector of user revoca- tion tokens grt, similarly indexed,
(gsk, grt) ← KeyGen(1k, n)

2) Sign(gpk, gsk[i],M): This randomized algorithm takes as input the a private key gsk[i],group public key (gpk), and a message $M \in \{0, 1\}*$, and returns a signature σ.
$\sigma t \leftarrow Sign(gpk, gsk[s], C(t1), Ct, t)$

3) Verify(gpk,RL, σ ,M): The verification algorithm takes as input the a set of re- vocation tokens RL whose elements form a subset of the elements of (grt), group public key gpk, and a claimed signature σ on a message M. It returns either valid message or invalid message. The latter response can either conclude that σ is not a valid signature, or that the user who generated it has been revoked.
$0, 1 \leftarrow Verify(gpk, RL, \sigma, M)$

4 SYSTEM ARCHITECTURE

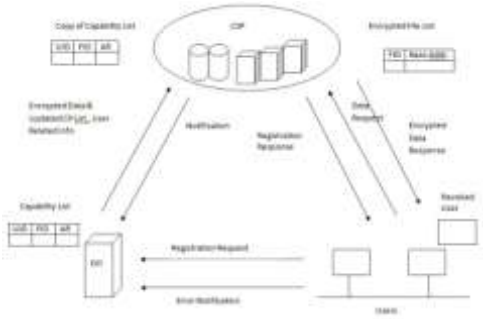

Fig. 1. System Architecture

The 1 describes the system architecture of the proposed system. The architecture consists of three different entities, namely, the Cloud Ser- vice Provider (CSP), the Data Owner (DO) and the Data Users, actually the group of users.

Data Owner is an entity who creates the data or a file. It has rights to grant access to the file depending on the user. It stores a list known as Capability List. Capability List as three fields namely, User Identity (UID), File Identity (FID), and the Access Rights (AR). It uploads the created file on cloud in encrypted format. It sends the copy of the capability list to the CSP.

Cloud Service Provider is an entity which provides service to the users. It provides access to the files uploaded on cloud. It has a copy of the capability list which is used to check the access rights of all users. Based on the access rights the file request is processed by it. It also has a Encrypted File List, which consist of File Identity (FID) and the base address of the file.

Users are the entities which uses the services provided by the CSP. Before using the service, they must register themselves to the DO. Users can request for the file for which they have access. They receive the requested file from the DO in encrypted format. File can be decrypted by the user when the threshold number of users provides their part of the key. Revoked user is the new user in the group.

5 IMPLEMENTATION DETAILS

5.1 SOFTWARE SPECIFICATIONS

For implementation we have used :

1) Coding Platform: Java
2) IDE : Eclipse
3) Database : MySQL

5.2 MATHEMATICAL MODEL

Set Theory: Let S be the system object It consist of following Where S={I,P,O} S denoted the System which consists of the following ,

I = Input
P = Process
O = Output

1. Input, I={U,F,CL}

U={u1,u2,u3,..un} that is users can be infinite.
F={f1,f2,f3,..fn} and files can be infinite.
CL=Capability List

2. Process, P={ P1, P2, P3, P4, P5}

P1 = Process is carried out to ensure data confidentiality DO and CSP and, authentication of DO and CSP.
P2 = Process which DO and CSP apply after a new file creation in respect.
P3 = Process ensures secure communication of data between CSP and user.
P4 = This process includes threshold cryptography technique for decryption of a users file.
P5 = This process is carried out to handle User Revocation.

3. Output, O = {Success, Fail}

Success = User can decrypt the file if he has the proper access right as well as key part of threshold number of users.

Fail = User cannot decrypt the file if he does not have proper access right or key part of less users than the threshold number of users.

6 EXPERIMENTAL RESULTS

The figures include in this section describes some functions provided by the system. The output of the system will ensure the confidentiality, integrity and access control of the data files uploaded on the cloud. The users must get the requested data if he has the proper access control on that file. Threshold number of users will provide their keys to decrypt and use the requested file. System is useful for the functions which work in group of users. System ensures reduction of number of keys required and also manages the user revocation. New user can easily work with the group as well as group can still perform operations even after a group member gets removed from the group.

Fig. 2. User's Login Page

Fig.3. User's Profile Page

Fig. 4. List of Files Uploaded on Cloud

Fig. 5. Page to Upload Files on Cloud

7 CONCLUSION

Security for information outsourced at CSP is ensured by the proposed system. Some methodologies are given to secure outsourced information yet they are experiencing having huge number of keys and intrigue assault. By utilizing the threshold cryptography at the client side, outsourced information is shield from agreement assault. Since, DO stores its information at CSP in scrambled frame and, keys are known just to DO and regarded clients bunch, information confidentiality is guaranteed. To guarantee fine-grained access control of outsourced information, the plan has utilized ability list. Open key cryptography and MD5 guarantee the element verification and information integrity individually. Open

key cryptography and D-H trade shielded the information from untouchables in this methodology. No of keys (on the grounds that in threshold cryptography, there is a single key comparing to every gathering)have decreased in the pro- posed plan. Even the proposed scheme man- ages the functioning in case of user revocation.

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, 23-25 May 2011.

[2] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy, O'Reilly Media, Sep. 2009.

[3] 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.

[4] S. Sanka, C. Hota, and M. Rajarajan, Secure data access in cloud computing, Internet Multimedia Services Architec- ture and application (IMSAA), 2010 IEEE 4th International Conference on, vol., no., pp.1-6, 15-17 Dec. 2010.

[5] 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: 01Issue: 01 Page:(2011).

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, Im- proved proxy re-encryption schemes with applications to secure distributed storage, in Proc. of NDSS05, 2005.

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

[8] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, Over-encryption: Management of access con- trol evolution on outsourced data, in Proc. of VLDB07, 2007.207.

[9] Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats, Threshold Cryptography Based Data Security in Cloud Computing, 2015 IEEE International Con- ference on Computational Intelligence Communication Technology.

[10] A. Shamir, How to share a secret, Communications of theACM, v.22 n.11, p.612-613, Nov. 1979.

Nikeetaa Choudharri She is currently pur- suing Masters Degree in Computers at RMD Sinhgad School of Engineering. She has completed her Bachelor's Degree at Universal COE from Savitribai Phule Pune University.

Ms. Kanchan Varpe She is currently working as an Assistant Professor at the Department of Computer Engineering of RMD Sinhgad School of Engineering,Pune. She is having around 8 years of experience in teaching. She has completed her Masters Degree in Computer Networks.