Secure Threshold Cryptography Based Data security system in multi-owner architecture.

Sagar Rakshe , Sachin Tandale , Rushikesh Suryawanshi , Onkar Thorawade

Guided by :- Prof. Pallavi Yevale
(Department of Computer Engineering,SKNSITS,Lonavala)

Abstract

Cloud computing has became a very popular service which can offer number of online services as well as online storage of data at low price. Other than these highly advance service there are number challenges like data confidentiality, data integrity and access control of data. There are some approaches which are previously suggested for data security but they aren't that reliable and feasible as in there are chances of data violation due to collision attack and heavy computation. To minimize this issues a proposed system this uses threshold cryptography in which data owner Divides users in groups and gives a single key to each user group for decryption of data, and each user in the group shares the parts of the key. There a re multiple owners of keys in this proposed system. There is a onetime session password (OTP) which is shared between user group and data owner for authentication of users. The key is encrypted using Deffie-Hellman algorithm which provides us secure transaction of file.

Index Terms :- *Capability list, Threshold Cryptography,S-Hash,Authentication, Deffie-Hellman***.**

I. INTRODUCTION

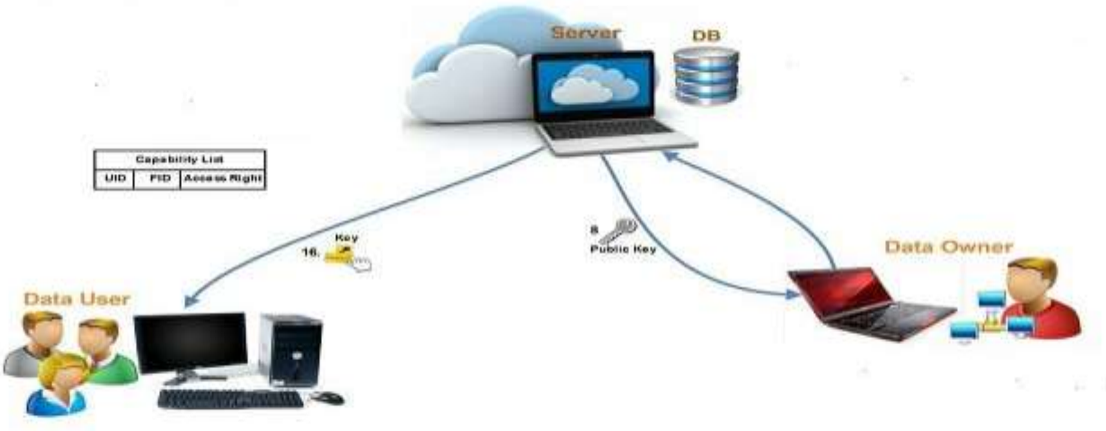
We live in a world of technology where every day we come across lots of intelligent or smart computer. As day by day the main frame computer are been reduced to small size and made affordable to common people. To tackle problem of storage and security for user data cloud computing was introduced. Cloud user stores their sensitive data to the cloud. Thus it becomes cloud serv ice provider’s responsibility to establish secure communication mechanism. It should provide secure channels for sending and receiving data and also for storing data. Thus security is big concern to cloud service providers. Current research work offe rs sharing with security. Service providers use different encryption decryption algorithms for secure communication and storage of data.It provide basically services like PaaS (Platform as a service), IaaS (Infrastructure as a service), SaaS (Software as a service).Users have right to access data from any part of the world and store data over it. There are various type of service provide by cloud like public, private, personal or hybrid the user can choose according to its need. Due to security provided as service by cloud many of institute and companies are exploring cloud and moving their business over it. But the problem with cloud computing is that people don’t trust cloud for storing their data as leaking the data can result loss in confidentialit y of the industrial data. Many data securing scheme were introduce but they are suffering from data collision of malicious user and heavy computation. To overcome this Problem of heavy computation and data collision Access Control List (ACL) has been introduced which specifies the user right and permit permission accordingly. Deffie-Hellman algorithm has been used in this to generate session key or one time password. S-hash algorithm has been used for Encryption and Decryption of data.

II .PROPOSED SYSTEM

This model is composed of three entities :a CSP, a DO and many users along with DO. Initially all users are registered at DO. During registration users send their credentials to DO. First data owner login to their respected sy stem and then select capability list ,file to upload and team leader. Then DO encrypt file using their his private key and then calculate the hash of that private key. This calculated hash of private key is then encrypted using another key. Here AES algorithm is used encryption purposed. File is encrypted using hash key and then hash of file is also calculated. After encryption processs by AES algorithm , request is sent to cloud service provider for uploading of file.

At CSP side, send his public key to DO. Then DO encrypts file using public key of CSP by using RSA algorithm.and then finally file is uploaded to server.CSP then decrypts file using his private key using RSA algorithm. Database of CSP stored hash of t he file, Encrypted file and encryption key.

Data users then registered to systemand select file which is to be download. At the same time at CSP OTP(one time password) is generated mail to to all registered users account and keys are send to each data user using Diffie -hellman algorithm. All users then entered their respected keys and decrypts file.



There are total four algorithms in the proposed scheme. Algorithm 1 which describes secure communication of data between DO and CSP . Algorithm 2 which describes procedures which DO and CSP apply after a new file creation in respect. Algorithm 3 describes the secure communication of data between User and CSP. Last Algorithm 4 which 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 and no threat of collusion attack as in group-key scheme.

Algorithm 1:Procedure to be followed by CSP after getting

Step 1: CSP stores Encrypted Data and Capability List which are received from DO Array ← Rece(EkPbCSP(EuPkDO ((Fl)) || (CList))
(Fl) ← DuPkCSP(DuPbDO((Array))
Step 2: CSP updates the Encrypted File List Encptd. File List ← Encptd. File List (FID, Base Adds.)
Step 3: CSP updates Capability List CPList ← CPList(UID, FID, AR)

In Algorithm 1 , CSP decrypts a file using its own private key and public key of DO and stores rhe encrypted data and capability list in its storage and update capability list.

Algorithm2: Algorithm for secure data exchange between CSP and User by using Modified D-H key exchange

Step 1: User sends data access request to CSP.
Send UID, FID and AR
Step 2: CSP matches UID, FID, AR with CList stored at it.
If(match) Go to step (3) else Go to step (6)
Step 3: CSP initiate D-H exchange with that User and shares one time shared session key(OTP)
Step 4: CSP encrypts the encrypted File with shared one time session key and sends it to User Send
Step 5: User decrypts File and calculates msg digest of that File If Calculated digest matches with stored digest then File is original else File is modified and User sends Error Notification to DO
Step 6: CSP sends 'invalid request' message to User

Algorithm2 describe how data are exchange securely among CSP and the Users by use of modified Diffie -hellman algorithm. CSP initiates D-H exchange with user and shares one time shared session key(Kp).

Symbol	**Description**
DO	Data Owner
CSP	Cloud Service Provider
Pk	Private Key
Pt	Public Key
Sk	Symmetric key
Eu	Encryption
Du	Decryption
PCSP	Public key of CSP
PCSP	Private key of CSP
PDO	Public key of DO
PDO	Private key of DO
PUSR	Public key of USER
PUSR	Private key of USER
FID	File Identity
UID	User Identity
Kp	Secrete Session Key
Xa/b	Chosen Secret Key
Ya/b	Calculated Public Key

LIMITATION AND SCOPE FOR FUTURE RESEARCH

In proposed system, we distribute key among the users so there is increase the maintenance of security of each key. Also it is used where there is team or group work. In the future we can include data tempering identification system in it.

CONCLUSION

The prime objective of our survey paper is to find out an efficient and effective way of transfer of file through server by using Symmetric or Asymmetric algorithm. The different algorithms used suffered from collision of data or high time complexity which result in failure of providing the basic necessity of security to file so to overcome this failure a hybrid algorithm should be introduce which would help in proper distribution of keys along the authenticate user.

REFERENCES

[1] 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

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

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

[4] S. M. Metev and V. P. Veiko, Laser Assisted Micro technology, 2015.2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[5] J. Breckling, Ed., and the Analysis of Directional Time Series:Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[6] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, ―A novel Ultrathin elevated channel low-temperature poly-Si TFT,‖ IEEE Electron Device Lett. vol. 20, pp. 569–571, Nov. 1999.