Two End point Verification of secure Data storage over Cloud

[1]Lankalapalli Bhargava, [2]KunaVenkataKiran
[1]*Final M.Tech Student,*[2]*Assistant professor*
[1,2]*Dept of CSE, Kaushik College of engineering Visakhapatnam., Andhra Pradesh, India.*

Abstract:

We are proposing an empirical model of out sourcing of information to multiple data owners with secure key generation and two level authentication process, one is over data owners and other is over key generation center. Initially data owner level authentication cane performed with secret key and random challenges and followed by key generation process and after reconstruction of the key generation center also authenticated with signature or hash code. Shamir secret sharing technique can be used for secure key generation

Index terms: multi owner data sharing, group key management, cryptography

I. INTRODUCTION

Now a days sharing of data is useful feature to get the information shared among different users with low expenses and efficient data transfer, in order to satisfy the above mentioned feature a vital cloud computing technique is proposed. Multiple data sharing is always a introduce a challenge of privacy over the data share at the cloud due to unknown users using the data at the same time by different users so to overcome this a new approach is introduced multiple data sharing technique for a dynamically added group of people over the cloud.by applying the signature and encryption of the data of the user can identify the specific user and also provide the privacy and security of the data over the cloud technology by the anonymous users. Encryption reduces the expense of the user data storing with other user storing them and retrieving the information without getting conflict with the other users.

Cloud computing replaces the long established information technology with in no time with its effects and advantages of low expenses and basic resource of data transformation there are many service providers which provide the data sharing with the high efficient data sharing centers to provide the privacy and security of the data over the cloud. Data transferring plays a vital role but huge data sharing is not possible all the time without the break so to overcome this providing the data at a cloud which is accessible without moving it from place to place this place a significant feature in data sharing over the cloud

In traditional approach handling multi owner data sharing is a complex issue, various researchers proposed various approaches for the problem, previous approaches divides the files into number of blocks and applies cryptographic mechanism over individual blocks, it is very time complexity process and while addition of new owner again key should be updated and it should be accepted by the all data owners.

- Simple Symmetric and Asymmetric Cryptographic techniques cannot maintain the optimal security
- It is vulnerable ,if transfers the key directly over network
- Authentication of data owner is not integrated in traditional approach

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.
Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

II. RELATED WORK

Consider an example of a company with employees divide by departments while one department may not know details of all the employees but by using the cloud employees can be released the troublesome of the data storing and maintenance of the data over the cloud computing.Cloud providers provide the cloud service to manage the data of the user without any conflict with the other users because of the data confidentiality of the users and also sensitivity of the data.so to prevent the data mislead or leaked a

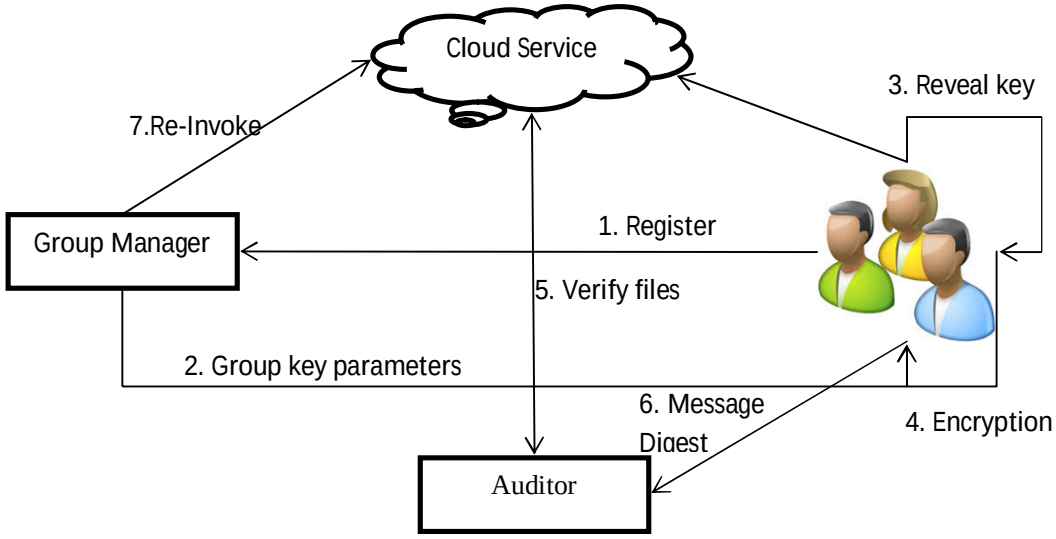
simple encryption is used and upload the data over the cloud to over the mislead of the data

In cloud computing the confidentiality of data plays an important role because users need to know the level of security of their data without having a clear understanding over thedata sharing over cloud user may not be in a position take the use of the cloud computing, in order to know whether the service provider reveal the data of one user to the other because they don't want to reveal the information data. Membership of the user is to provide efficient for updating the secret key for the left over user to reduce the complexity of data sharing over the clod in management of key over the unsecured data share of the user .so these approaches are used to get the data protect from the service provider and also from the service along with the unrecognized user for the data to be shared over the network in the cloud using the encryption technique for the file or the data stored by the specific user and get the security and also the service with quality.

Every Group Member forwards a random challenge (R_i) to group manager, in turn it forward a secret share (x_i,y_i),data member computes (x_i, (y_i XOR R_i)) and forwards the verification share to group manager and group manager verifies the user authentication with reverse XOP operation with random challenge, if it generates the corresponding member secret share ,then member is an authorized member

III. PROPOSED WORK

The proposed system identified the problems during multi owner data sharing and proposed an efficient protocol and cryptographic technique for solving drawbacks in the traditional approach. It proposed an efficient and novel secure key protocol for group key generation, new user need not to contact the data owner during the downloading of files and data can be encrypted with Triple DES before uploading the data in to the cloud. The proposed work involves the modules as Data owner, Group key manager and user revocation and the architecture as below



Improved lagrangeous polynomial group key scheme:

In this scheme, any t out of n shares may be used to recover the secret. The system relies on the idea that you can fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. It takes two points to define a straight line, three points to fully define a quadratic the four points to define a cubic curveand so on. That is it takes t points to define a polynomial of degree t-1. The method is to create a polynomial of degree t-1 with the secret as the first coefficient and the remaining coefficients picked at random. Next find n points on the curve and give one to each of the players. When at least t out of the n players reveal their points, there is sufficient information to fit a $(t-1)^{th}$ degree polynomial to them the first coefficient being the secret.

Algorithm:

- Goal is to divide some data *D* (e.g., the safe combination) into n pieces D_1,D_2….D_n in such a way that:

  - Knowledge of any k or more D pieces makes D easily computable.
  - Knowledge of anyk -1 or fewer pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is called (k,n) threshold scheme. If k=n then all participants are required together to reconstruct the secret.
- Suppose we want to use (k,n) threshold scheme to share our secret S where $k < n$.
- Choose at random (k-1) coefficients $a_1,a_2,a_3 \ldots a_{k-1}$, and let S be the a_0
  $f(x)=a_0 + a_1x + a_2x^2 + \ldots\ldots\ldots + a_{k-1}^{k-1}$
- Construct n points (i,f(i)) where i=1,2…..n

Recall that the secret is the free coefficient, which means that S=1234.

After getting group key to data owner's data owners are able upload data. The data is to be encrypted and upload encrypted data. All data owners encrypt their data using Triple DES algorithm. It is shown below.

TDES is a block cipher operating on 64-bit data blocks. Some forms of TDES use two 56-bit keys, while others use three. TDES can however work with one, two or three 56-bit keys. The parallel implementation improves performance and reduces gate count.

Algorithm:

Map n-bit plaintext blocks to n-bit cipher text blocks (n = block length).

• For n-bit plaintext and cipher text blocks and a fixed key the encryption function is a bi-ejection;

• $E : P_n \times K \rightarrow C_n$ s.t. for all key $k \in K$, $E(x, k)$ is an invertible mapping, written $E_k(x)$.

• The inverse mapping is the decryption function, $y = D_k(x)$ denotes the decryption of plaintext x under k.

Block size: in general larger block sizes mean greater security.

• Key size: larger key size means greater security (larger key space).

• Number of rounds: multiple rounds offer increasing security.

• Encryption modes: define how messages larger than the block size are encrypted, very important for the security of the encrypted message.

The F-function, depicted in Figure 2, operates on half a block (32 bits) at a time and consists of four stages:

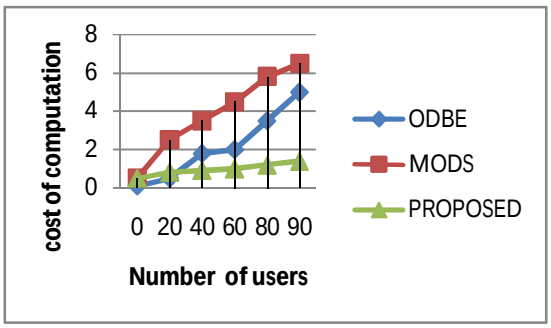
1. *Expansion* — the 32-bit half-block is expanded to 48 bits using the*expansion permutation*, denoted *E* in the diagram, by duplicating half of the bits. The output consists of eight 6-bit (8 * 6 = 48 bits) pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side.
2. *Key mixing* — the result is combined with a *subkey* using an XOR operation. 16 48-bit subkeys — one for each round — are derived from the main key using the *key schedule* (described below).
3. *Substitution* — after mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the *S-boxes*, or *substitution boxes*. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES — without them, the cipher would be linear, and trivially breakable.
4. *Permutation* — finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the *P-box*. This is designed so that, after permutation, each S-box's output bits are spread across 4 different S boxes in the next round.

IV. EXPERIMEETAL ANALYSIS

Given any subset of k of these pairs, we can find the coefficients of the polynomial by interpolation, and then evaluate a0=S , which is the secret.

Example:

- Let S=1234
- n=6 and k=3 and obtain random integers a_1=166 and a_2=94
  $f(x)=1234+166x+94x^2$
- Secret share points (1,1494),(2,1942)(3,2598)(4,3402)(5,4414)(6,5614)
- We give each participant a different single point (both x and f(x)).



Re-construction:

- In order to reconstruct the secret any 3 points will be enough
- Let us consider

$(x_0,y_0)=(2,1924),(x_1,y_1)=(4,3402),(x_2,y_2)=(5,4414)$

Using lagrangeous polynomials

$L_0=x-x_1/x_0-x_1*x-x_2/x_0-x_2=x-4/2-4*x-5/2-5=(1/6)x^2-(3/2)x+10/3$
$L_{1=}x-x_0/x_1-x_0*x-x_2/x_1-x_2=x-2/4-2*x-5/4-5=-(1/2)x^2-(7/2)x-5$
$L_2=x-x_0/x_2-x_0*x-x_1/x_2-x_1=x-2/5-2*x-4/5-4=(1/3)x^2-2x+8/3$
$f(x)=\sum_{j=0}^{2} y_j l_j(x)=1942((1/6)x^2-(3/2)x+10/3)+3402(-(1/2)x^2-(7/2)x-)+4414((1/3)x^2-2x+8/3)$
$f(x)=1234+166x+94x^2$

The above graph shows the efficiency of proposed work comparison with previous methods. Our work efficiently reduces the calculation complexity while revealing the key. ODBE and MODS are more complex in nature and processing time also increases for more number of members in a group.

V.CONCLUSION

In this paper, we design a secure data sharing scheme for dynamic groups in an third party cloud. A user is used to share data with others in the group without revealing identity privacy to the cloud. It gives efficient user revocation and new user joining. User revocation can be achieved through a public revocation list without updating the private keys of the remaining users and new users can directly decrypt files stored in the cloud before their participation. The encryption computation cost is moderate. Extensive analyses show that our proposed scheme satisfies the desired security requirements.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
[2] Amazon Web Services (AWS), Online at http://aws. amazon.com.[3] Google App Engine, Online at http://code.google.com/appengine/.
[4] Microsoft Azure, http://www.microsoft.com/azure/.
[5] 104th United States Congress, "Health Insurance Portability and Accountability
Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.
[6] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy insecure groups," in Proc. of NDSS'01, 2001.
[7] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002.
[8] T. Yu and M. Winslett, "A unified scheme for resource protection inautomated trust negotiation," in Proc. of SP'03, 2003.
[9] J. Li, N. Li, and W. H. Wins borough, "Automated trust negotiationusing cryptographic credentials," in Proc. of CCS'05, 2005.
[10] J. Anderson, "Computer Security Technology Planning Study," AirForce Electronic Systems Division, Report ESD-TR-73-51, 1972,

BIOGRAPHIES

Lankalapalli Bhargava completed B.tech in lendi institute of engineering and technology. He pursuing computer science and engineeringin Kaushik College of engineering academic years.

KunaVenkata Kiranworking as Assistant professorin Computer Science&Engineeringdepartment in Kaushik college of Engineering, Visakhapatnam., AndhraPradesh, India. He pursued his B.Techfrom M.V.G.R CollegeandM.Techfrom Acharya Nagarjuna University. His research areas include Computer Networks & Security and Data mining.Currently He is associated with assisting of various academic projects among various fields with 5 years of teaching experience and 2 years of industrial experience. To his credit 7 international publications, 2 national publications and 4 workshops .Now he is guiding 5 U.G level and 2 P.G level projects