Optimal Data Sharing with Forward Security

Deepika V. Shinde
PG Department
MBES's College of Engineering
Ambajogai, India, 431 517.

B. M. Patil
PG Department
MBES's College of Engineering
Ambajogai, India, 431 517..

ABSTRACT
Cloud Computing is one of the best platform which provides huge data storage and data sharing all over the time and also easily available to the users. Data sharing in the cloud contains the several issues such as data integrity, authenticity, anonymity and privacy of data owner. Identity based (ID-based) ring signature gives anonymous and authentic data sharing system, by using this there is no need of costly certificate verification in the traditional public key infrastructure (PKI).This work, enhances the security of ID-based ring signature with forward security. Using forward security, if private key of the signer is compromised then all the previously generated signatures of that signer remains valid.Using forward security, one of the user may revoke access of file to the other members of the group.

Keywords
Cloud Computing, data sharing, data integrity, data authenticity, ring signature, anonymity, forward security.

1. INTRODUCTION
Cloud computing is an emerging technology and it is a internet based technology that gives shared computer processing resources and information to computers and other devices on demand. Sharing of data is very important in cloud computing and providing security to that data is also important.Along with the data sharing, data integrity is also need to be maintained. Ring signature provides authentic and anonymous data sharing system so that any member in the ring can keep his data secretly into the cloud for storage and analysis purpose. Ring signature requires verification of public key certificates which is both time and cost consuming so this is the bottleneck for ring signature.

Data sharing in cloud computing contains the several issues such as:

- Data Authenticity: In cloud data is gathered from number of external resources so it is necessary to provide security to that data.This usage of data would be misleading if it is forged by adversaries.
- Anonymity: In the cloud, numbers of users are more so it is difficult to prevent identity of each user while using the data in cloud.
- Data Integrity: In the cloud any user can access the data easily which is available in cloud so it is difficult to maintain accuracy and consistency of data.

1.1 Id Based Ring Signature
Using Identity based (ID based) cryptosystem there is no need for verification of validity of public key certificates.In this ID based cryptosystem, public key of each user is computed from a string corresponding to the users publicly known identity.Private keys are computed from its master secret for users by a private key generator(PKG).Thus verification of public key certificates is eliminated.
Ring signature is a group of n number of users with the privacy protection on signature creator.Any user can sign on behalf of a group anonymously while other group members are totally unaware of it.Here identity of the signer is hidden from other group members so any verifier from group members is convinced that a message has been signed by one of the groupmember in the ring.

ID-based ring signature has a significant advantage in big data sharing system.Let us consider one example.In traditional public key ring signature suppose there are 30000 members in the ring then 30000 public key certificates are validated to the corresponding members by the verifier, after which one can carry out the actual verification on the message and signature pair.On the other side, in ID based ring signature only identities of ring members together with pair of message and signature are needed.

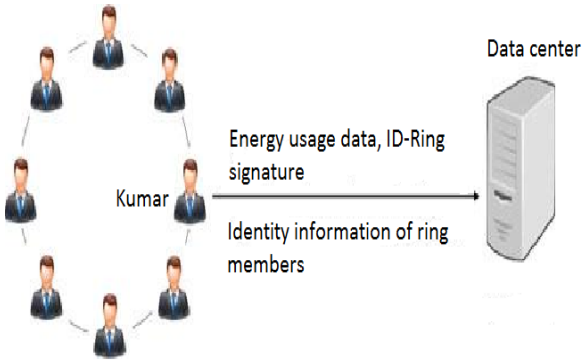

Figure 1.A Solution based on ID-based Ring Signature [11]

As shown in Figure 1, ID-based ring signature is most usable where large numbers of users are present.

- Step 1: The data owner(say Kumar) first setups a ring by choosing a group of members.it only needs the public identity information of ring members, such as residential addresses and Kumar does not need agreement from any ring members.
- Step 2: Along with ring signature and identity information of all ring members, Kumar uploads his data also.
- Step 3: By verifying the ring signature, one can assure that data is taken out by a valid member from the ring while the member it is hidden.Hence anonymity of the data owner is maintained along with the data authenticity.And also this process does not involve any certificate verification.

1.2 Key Exposure

ID-based ring signature provides data sharing with large number of participants.To provide higher level protection to the data one can add more users in the ring, this may include chances of key exposure.Key exposure is major limitation of ID-based ring signature i.e. if key of signer is exposed then all the previously generated signatures are invalidated and are not trusted anymore.Also its future signatures are also rejected.Key recovery mechanism is also started using compromised private key but it does not solve the problem of past signatures.

The issue of key exposure in big data sharing system is more severe in ring signature.If ring members private key is exposed, the rivals may generate valid ring signatures of any documents on behalf of that group.The opponents may include the compromised user in the group of his choice.So that exposure of one of the users private key invalidate all the previously generated signatures,since no one can identify whether a ring signature is generated is generated prior to the key exposure or by which user.Thus forward security was proposed to prevent all the previously generated or past signatures.

We use the following concepts to achieve the results

- ID-based ring signature with forward security formed, eliminates the use of costly certificate verification which makes it more suitable for big data sharing system.
- Uses AES algorithm for encryption/decryption of data of data owner.
- Uses SHA 512 algorithm to provide security to the data available in the cloud.

2. LITERATURE SURVEY

The ring signature scheme was introduced by Rivest et al. [2].In this scheme every ring member needs to verify the validity of public key certificates which is very costly. Bresson [3] extended the ring signature scheme into a threshold ring signature scheme using concept of partitioning.The first ID-based ring signature scheme was developed in 2002 which can be proven secure in random oracle model[5].using this all the users have their corresponding public key before their enrollment.ID-based cryptosystem proposed by Shamir, using this there is no need for verifying the validity of public key certificates.

Two constructions in the standard model was introduced by Au et al. [4].it mainly focus on data authenticity and anonymity.The first construction introduced by Ferrara focuses on the batch verification i.e. algorithm for digital signature scheme that verifies a list of n(message,signature) pairs as a group[6].While the second construction is proven secure in a weaker model namely selective ID model.The first ID-based ring signature scheme owned to be secure in the standard model by Han under the trusted setup assumption [9].Tsang point out the above proof is wrong and increased security in ID-based ring signature,which is essential for time reducing, cost effective authentic and anonymous data.

In ID-based ring signature, no one has provided the solution on the problem of key exposure i.e. previously signed all the signatures are eliminated.The solutions on this i.e. forward secure signature were designed by Bellare and Miner [3] and the concept was given by Anderson [1].It preserves the validity of past signatures even if the current secret key is compromised. Kong et al. provided security on multi cloud architectures using forward secure digital signatures [7] and they have also given the idea of forward secure ID-based ring signature, it is very important tool for building cost effective authentic and anonymous data sharing system [8].

3. PROPOSED SYSYTEM ARCHITECTURE

Using ID-based ring signature with forward security in the cloud,data sharing should be done in well-organized manner with security. The proposed system architecture is shown in figure 2. Clients in below figure represents individual cloud utilizers, they can store or download data in the cloud.Cloud servers may reside in different physical locations.Storage of data is decided by CSP depending upon available spaces in the cloud server.ID-based ring signature forms the ring of users i.e. all the users present in the ring are authenticated users.The secure data transfer is performed with different encryption and decryption techniques.

The components of system are CSP (Cloud Storage Service Provider), TTP (Trusted Third Party), and Data Owner and Authenticate user.

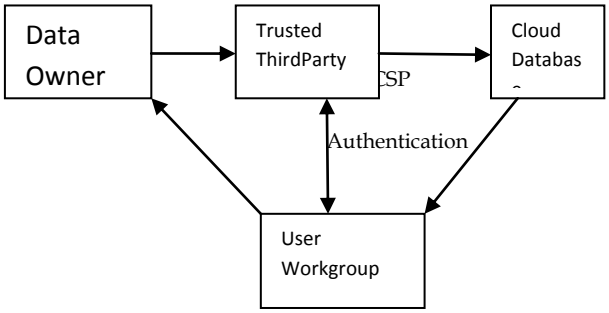

Figure 2.Proposed System Architecture

- Data Owner: If data owner wants to store and share data over cloud then his information will be stored on cloud by CSP.Data owner wants his data to be secure i.e. not observable to CSP so TTP is used. Data is encrypted before uploading and kept at TTP.
- Trusted Third Party(TTP): Data at TTP requires regular audit for security purpose.Database Administrators(DBA) set up regular auditing that involves the actions related to the database.Auditing is the process of monitoring and recording of user selected database activities .they can collect the data related with authorization and access control execution.DBA can also collect the data about which tables are need to be changed, how many logical I/O operations are carried out or how many current user can be connected at real time.
- Authentic User: Authenticate user is one of the client of data owner. He has all the rights to access the information in the cloud. User have to register itself to become a group member.
- Cloud Storage Service Provider (CSP): CSP allows data owner to keep any type of the data in the cloud.According to the available data or user requirement the space for data will be allocated by the CSP.

4. FORWARD SECURITY MODEL

ID-based Forward Secure Ring Signature (IDFSRS) scheme consists of following probabilistic polynomial time (PPT) algorithms:

1) Setup: By giving an unary string as input where a security parameter is considered as λ , the algorithm generates a master secret key msk for the third party PKG (Private Key Generator) along with a list of system parameters param that includes λ and the information of a user secret key space D, a message space M and signature space S.

2) Extract: On input a list of system parameters,an identity $ID_i$for a user and the master secret key msk, the master secret key msk,the algorithm outputs the users secret key $sk_{i,0}$ ε D such that the secret key is valid for time t=0.

3) Update: On input a user secret key $sk_{i,t}$ for a time period t, the algorithm gives $sk_{i,t+1}$ as a new user's secret key for time period t+1.

4) Sign: On input a list param of system parameters, a time period t,a group size n of n user identities,a message m ε M, and a secret key for time period t,the algorithm outputs a signature.

5) Verify: On input a list param of system parameters,a time period t,n group size , n user identities,a message m ε M,a signature that belongs to S, it outputs either valid or invalid.

5. ALGORITHM

Here we use AES 16-bit algorithm for encryption/decryption purpose and SHA-512 algorithm to provide security to the data present in the cloud.

5.1 AES 16-Bit Algorithm

Generate user u1 ID; Set of users u1's attribute i.e. Domain B;

Domain manager checks all the attributes;

Now, Generate RandomValue [unique] attribute = k;

Generate Random value [user] =r1;

Secret key = (k+r1).user u1's ID;

Encrypting user data along with ID;

Encrypt (user ID. (k+r1)+data);

Decrypting user data along with ID;

Decrypt (user ID. (j+r1)+data).

5.2 Sha 512 Algorithm

Input: string required to calculate the SHA score.

Output: SHA score of string.

Step 1: Padded with the length in such a way that the result is should be in multiples of at least 512 bit long in size.

Step 2: divide stream into 512 bit message blocks M(1),M(2)…….M (n) the message block can process at a time using the starting hash values H (0).

Step 3: Then compute the sequence

$$H(i) = H(1)+CM(i) (H(i1)) \quad \text{----------(I)}$$

Step 4: return the H(i) SHA score of given string.

6. RESULT AND DISCUSSION

For the proposed system performance evaluation, we deploy the system on java 3-tier MVC architecture framework with INTEL 3.0 GHz i7 processor and 8 GB RAM.We deploy the system on EC2 public cloud with single virtual machine (VM).Here each graph shows the system performance with different experiments that has been classified in graphs.

Here the graph shown below is the graph for file uploading time i.e. time required by the user to sign a file and secret key generation for the user. Here time required to upload last five files is considered and generated graph showing result for this.Here x = File length (in bytes) and y = File uploading time.

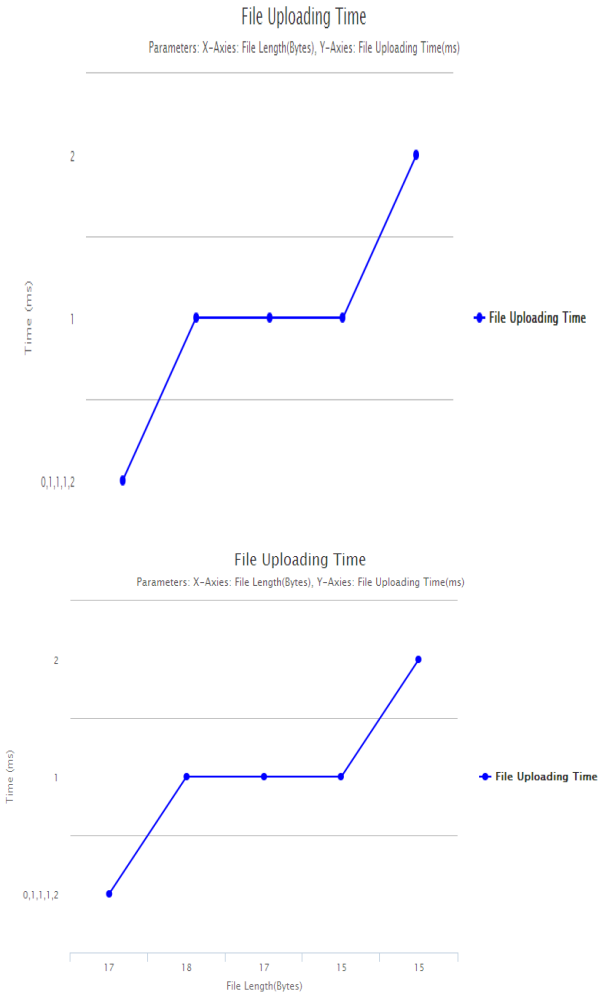

Figure 3.File Uploading Time

Second graph shown below is the graph for file downloading i.e. time required by the user for verification and file download time. Here also time required to download last five files is considered and generated graph showing result for this.Here x = File length (in bytes) and y = file downloading time.

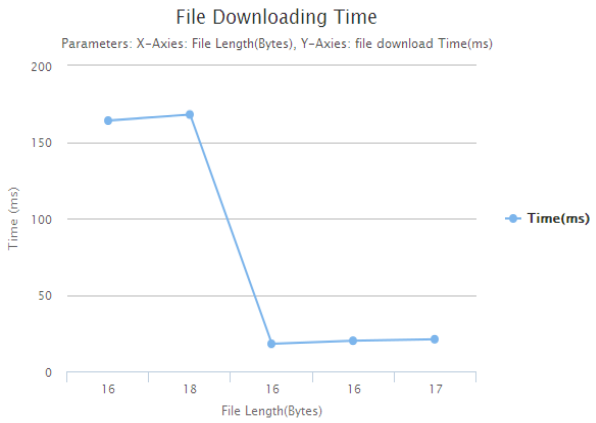

Figure 4.File Downloading Time

Next graph shown below is the comparison graph for ID-based ring signature and ID-based ring signature with forward security.When any user revoke the access of a particular file to other user then in ID-based ring signature all the previously uploaded files access is restricted and in ID-basedring signature with forward security only access to the current file is restricted.

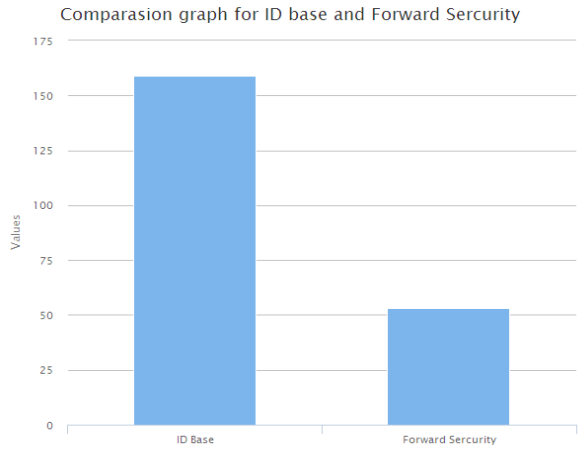

Figure 5. Comparison Graph for ID-Based and Forward Security

7. CONCLUSION

We discussed ID-based forward security which provides unconditional anonymity and it does not require any matching operation.. By using AES algorithm size of secret key is reduced and update of key process is easy. Our scheme is very useful in many practical applications, especially where user privacy and authentication is required, such as ad-hoc network, smart grid. e-contract signing, e-auction etc. Our scheme also provides more security to the data available in the cloud. A secure scheme with same features in standard model can be considered as an open problem and in future research work. We can also use this scheme in future for multi-cloud framework.

8. REFERENCES

[1] R. Anderson. Two remarks on public-key cryptology. Manuscript, Sep. 2000. Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.

[2] M. Klonowski, L. Krzywiecki, M. Kutylowski, and A. Lauks. Stepoutring signatures. In MFCS, volume 5162 of Lecture Notes inComputer Science, pages 431–442. Springer, 2008.

[3] M. Bellare and S. Miner. A forward-secure digital signaturescheme. In Crypto'99, volume 1666 of Lecture Notes in ComputerScience, pages 431–448. Springer-Verlag, 1999.

[4] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-basedring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

[5] F. Zhang and K. Kim. ID-Based Blind Signature and RingSignature from Pairings. In ASIACRYPT 2002, volume 2501 ofLecture Notes in Computer Science, pages 533–547. Springer, 2002.

[6] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen.Practical short signature batch verification. In CT-RSA, volume5473 of Lecture Notes in Computer Science, pages 309–324. Springer,2009. Full version appeared in http://eprint.iacr.org/2008/015.

[7] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forwardsecureidentity-based signature: Security notions and construction.Inf. Sci., 181(3):648–660, 2011.

[8] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo. Noninteractiveforward-secure threshold signature without randomoracles. J. Inf. Sci. Eng., 28(3):571–586, 2012.

[9] J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ringsignature scheme. In EUC (2), pages 437–442. IEEE ComputerSociety, 2008.

[10] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-basedring signature scheme secure in the standard model. In IWSEC,volume 4266 of Lecture Notes in Computer Science, pages 1–16.Springer, 2006.

[11] J. K. Liu, T. H. Yuen, and J. Zhou. Forward secure ring signature without random oracles. In ICICS, volume 7043 of Lecture Notes in Computer Science, pages 1–14. Springer, 2011.