Development of Cost-Effective Authentic and Anonymous Data Sharing system using Cryptographic Security Tools

Kajal[1], Sambodhi [2],Rashmi [3], Rohini[4]

[1] *Kajal R. Chauhan [B.E.], Information technology, Sanjivani COE, Kopargaon, Maharashtra, India.*
[2] *Sambodhi R. Gilche [B.E.], Information technology, Sanjivani COE, Kopargaon, Maharashtra, India.*
[3] *Rashmi R. Bhalerao [B.E.], Information technology, Sanjivani COE, Kopargaon, Maharashtra, India*
[4] *Rohini D. Mandwade [B.E.], Information technology, Sanjivani COE, Kopargaon, Maharashtra, India.*

ABSTRACT

Cloud computing moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. So there is a huge need to study the problem about data storage. Our proposed system is useful to reduce the computational cost at user side during the integrity verification of the data. Data sharing has never been easier with the advances of cloud computing. At the time of data sharing with a large number of participants must take into consideration several issues like efficiency, data integrity and privacy of data owner. For providing security to the system we proposed a scheme like Id-based Ring signature. It is a promising candidate to construct an anonymous and authentic data sharing system. It allows data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Identity-based (ID-based) ring signature eliminates the process of certificate verification. In the proposed system we will try to enhance the security of ID-based ring signature by providing forward security using cryptographic tools. If a secret key of any user has been compromised, all previous generated signatures including that user still remain valid. And this is especially useful to any large scaled at a sharing system. But one issue is still exists that, it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised. Hence, we have proposed to provide a security and efficient instantiation. Also it helps to provide security from reset attacks launched by the cloud Storage server in the upload phase.

Keyword : - Authentication, data sharing, cloud computing, forward security, smart grid.

1. INTRODUCTION

The Internet is involved in many new technologies. One of the most popular technology is cloud computing. Cloud computing environment provides the massive storages facility to the client. There are various types of data are stored in cloud computing environment. This new data storage. In cloud brings many challenging issues which have profound influence on the usability, reliability, scalability, security, and performance of the overall system. One of the biggest concerns with data storage is that of data integrity verification at untrusted servers.

Traditionally, entire data was retrieved from cloud and cryptographic techniques, hash values are used for integrity verification. But this is the wastage of cost, computation of user and communication resources. Cloud storage allows users to store their data and enjoy high quality of services. It enables highly scalable, on demand and only pay per use services to be easily consumed over the Internet on an as needed basis. Cloud stores data on remote machine, so necessary to need more security from unauthorized person. In order to overcome this problem, we have decided to implement cost effective authentic data sharing system using cryptographic tools. The clients concern about data security, data integrity and sharing data with specific band of men and women must be addressed. Suppose an example encrypting data on client machine and then storing the information to cloud storage server computing hash of the information on client machine. Client trying out the responsibility of sharing the trick key

about encryption with specific band of people nothing but new notion called forward secure ID-based ring signature. In this the size of user secret key is just one integer while the key update process only requires an exponentiation.

Fig -1: Energy usage data sharing in smart grid.

Cloud provides unlimited storage with reduced deployment cost. It has many advantages over local storage. Cloud server provides facility to store users data on a cloud. So users can upload their data on cloud and can access it without any additional burden of time, location, and cost. One of the strength of cloud computing is that data are being centralized and outsourced in clouds. This kind of outsourced storage in clouds has become a new profit growth point by providing a comparably low-cost, scalable, location independent platform for managing clients data. The Cloud Storage Service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients since their data or archives. In the situation of smart grid statistic energy usage data would be misleading if it is forged by adversaries. This issue can be solved by using cryptographic tools. (e.g. message authentication code or digital signatures) one may encounter additional difficulties when other issues are taken into account such as anonymity and efficiency. The number of users in a data sharing system could be HUGE (imagine a smart grid with a country size) and a practical system must reduce the computation and communication cost as much as possible. In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency such as:

1.1 Key Exposure in Big Data sharing System:

Forward secure ID-based Ring Signature and Authenticate have some advantages like Forward Security, Large Scale Data Sharing and it has limitations like Key Exposure in Big Data sharing System.

1.2 Unconditional Anonymity:

There are some properties like ID-based threshold ring signature and Identity escrow also some advantages like Identity-based Cryptography, Group oriented Cryptography and limitations like Unconditional Anonymity. Apply Identity-Based Ring Signature and IDBased Cryptosystem attributes for security using Trusted third party. Along with the cloud advantages security and integrity of data stored on cloud storage is burning issue. Users need to verify that their data remain as they stored on cloud, because data stored on cloud can easily be lost or corrupted due to human errors and hardware and software failures. Traditionally entire data was retrieved from cloud and cryptographic techniques, hash values are used for integrity verification. But this is the wastage of cost, computation

of user and communication resource user have to registered himself to the cloud server or to the third party which provide the cloud service. So the privacy of the data and security maintain by using encryption key and decryption key. In order to overcome the problem of integrity verification and security of cloud data many schemes are developed under different systems and models. Privacy of the user data and personal information can be provided by the cryptographic function and technology. And also proposes a new scheme i.e. Ring Signature Scheme, nothing but it is a group-oriented signature with privacy protection on signature producer. A user can sign anonymously on behalf of a group on his own choice while group members can be totally unaware of being conscripted in the group any verifier can be convinced that a message has been signed by one of the members in this group (also called the Rings) but the actual identity of the signer is hidden. A public verifier work as a Third-Party Auditor (TPA) to provide expert integrity checking services. public auditing mechanisms is used to verify shared data integrity ,that differently from traditional data storage, in cloud storage the data owner does not possess data physically after data is Out sourced into the Cloud Service Provider (CSP) who are not fully trusted. For the purpose of helping the data owner impose access control over data stored on untrusted cloud servers, a feasible consideration would be encrypting data through certain cryptographic primitives but disclosing decryption keys only to authorized users.

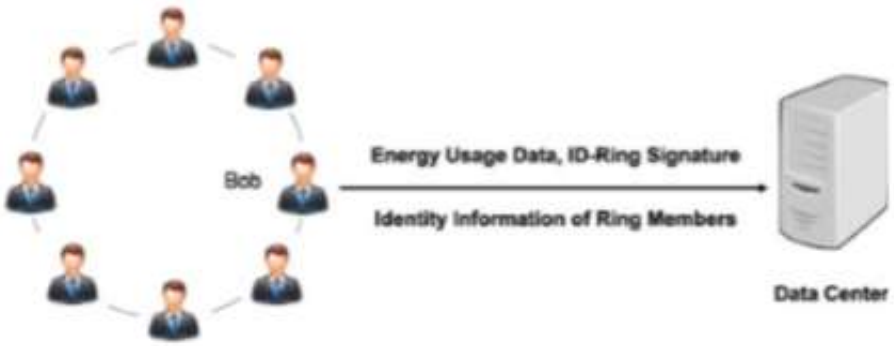

Fig -2: A solution based on ID-based ring signature.

However, this technique achieves security with less communication and computational overhead. Also developing a strengthened security model by considering the reset attack against the storage server in the upload phase of an integrity verification.

2. LITERATURE SURVEY

In this paper author have proposed a new ID-based ring signature scheme and a proxy ring signature scheme. This new and a proxy ring signature scheme, which whenever proxy signer want to sign message on behalf of the original signer provide anonymity. A ring signature is a simplified group signature without any manager. It protects the anonymity of a signer. It is based on RSA cryptosystem and certificate based public key setting. There are some properties like Forward secure ID-based Ring Signature and Authenticate also in that have some advantages like Forward Security, Large Scale Data Sharing and they have limitations like Key Exposure in Big Data sharing System. There are some properties like Forward secure ID-based Ring Signature and Authenticate also in that have some advantages like Forward Security, Large Scale Data Sharing and they have limitations like Key Exposure in Big Data sharing System. Identity-based (ID-based) cryptosystem introduced by Shamir eliminated the need for verifying the validity of public key certificate. These schemes also take care of the inconsistencies [1].

In recent years, ID-based ring signature schemes have been proposed and almost all of them are based on bilinear pairings. In this paper, author have proposed the first ID-based threshold ring signature scheme that is not based on bilinear pairings. Author have also proposed the first ID-based threshold 'linkable' ring signature scheme. Author emphasizes that the anonymity of the actual signers is maintained even against the private key generator (PKG) of the ID-based system. There are some properties like ID-based threshold ring signature and Identity escrow also in that have some advantages like Identity-based Cryptography, Group-oriented Cryptography and they have limitations like Unconditional Anonymity [2].

In this paper author introduces strong, formal definitions for the core requirements of anonymity as well as traceability of data. It is identical based formalization under which the adversary produces a message and a pair of group-member identities and returned a target signature of the given message. In this paper author proposes large set of ambiguous existing informal requirements in the literature for unifying and simplifying the requirements of the data. Ring signatures could be used for whistle blowing anonymous membership authentication for ad hoc groups and many other applications which do not want complicated group formation stage but require signer anonymity. A classical example like public-key encryption [3].

In this paper author proposes a multisignature scheme and a blind signature scheme. Both above schemes work is depend on Gap Diffie-Hellman (GDH) group. In this paper author proposes large set of ambiguous existing informal requirements in the literature for unifying and simplifying the requirements of the data. In this paper author proposes the following signature schemes. The new GDH threshold signature scheme. The new GDH multisignature scheme. The new GDH blind signature scheme. A classical example like "public-key encryption" [4]

3. EXISTING SYSTEM

There are so many applications and services moves to the centralized large data center where data may not fully trustworthy, to avoid this problem we are developing this forward security tools using cryptography. In our Proposed system issues of efficiency, data integrity, data confidentiality and privacy of data owner will get solved. This system has a two way communication one is a client side and another is a server side. whatever data get stored by user that can be saved in the encrypted format, while another user want to download his file then he might be known with his decryption key.

For providing security to the system we proposed a scheme like Id-based Ring signature. It is a promising candidate to construct an anonymous and authentic data sharing system. If a secret key of any user has been compromised, all previous generated signatures including that user still remain valid. And this is especially useful to any large scaled at a sharing system.

4. PROPOSED SYSTEM

To overcome the drawbacks of previous system or applications, we proposed an additional security for users. In our system architecture, there are two working sides. One is the client side and another one is the server side. When client sends request to the server, firstly that request is accepted by a TPA(Third Party Auditor). After that TPA detects whether the clients data is stored on cloud server or not. If yes, then TPA pass that request to the storage server. Then server audit that data to the TPA, then TPA delegate that data to the client and client will able to get his outsourced files. In the proposed system we will try to enhance the security of ID-based ring signature by providing forward security using cryptographic tools. If a secret key of any user has been compromised, all previous generated signatures including that user still remain valid. And this is especially useful to any large scaled at a sharing system. So there is a huge need to study the problem about data storage. Our proposed system is useful to reduce the computational cost at user side during the integrity verification of the data. Data sharing has never been easier with the advances of cloud computing.

Mainly four working parts are available in the architecture they are as follow:

4.1 Data owner:

Data owner is a user who owns data, and publishes to store it into the Storage Servers. The data owner also acts as the authority and is incharge of key generation. Information owner of the device component is the nothing but the user of desire to save and share data over cloud. Information owner isn't having any idea where my information will be stored by the CSP. Data owner store the data on cloud in encrypted format using encrypted key. Data owner share his encrypted key with TTP.

4.2 Trusted Third Party/Auditor:

When any of the client sends request to the server, that request firstly accepted by TPA. And he checks whether the sender is authenticated person or not. If yes then he provides authorization to access that remote data. Also TPA converts the data owners information in the encrypted form for security purpose

4.3 Authorized User:

Authorized User is a client of owner who has right to access the remote data.

4.4 Cloud Storage Service Provider(CSP):

Data base is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user defined database schema. It can be Non SQL / SQL form of database.

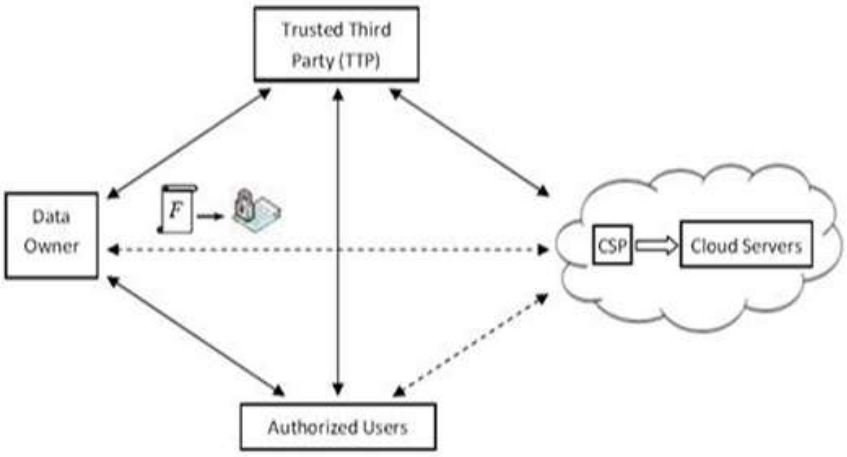

Fig -3: System Architecture.

5. IMPLIMENTATION

I propose a new notion called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system: For the rest time, system provide formal denitions on forward secure ID-based ring signatures; I present a concrete design of forward secure ID-based ring signature. No previous ID-based ringsignature schemes in the literature have the property of for-ward security, and rest to provide this feature; I prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption; and implementation is practical,in the following ways:

• It is in ID-based setting. The elimination of the costly certicate verication process makes it scalable and especially suitable for big data analytic environment.

• The size of a secret key is just one integer.

• Key update process only requires an exponentiation.

• System do not require any pairing in any stage.

5.1 Modules:

• Registration.

• Provided TTP.

• Data Owner Encryption.

• User Block.

• Attack Prevention.

• Resignature.

5.1Algorithm:

RSA encrypts messages through the following algorithm, which is divided into 3 steps :

1. Key Generation

I. Choose two distinct prime numbers p and q. II. Find n such that n = p q. n will be used as the modulus for both the public and private keys.

III. Find the totient of n, (n) (n) = (p-1)(q1).

IV. Choose an e such that 1 ¡ e ¡ (n), and such that e and (n) share no divisors other than 1 (e and (n) are relatively prime). e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation de 1 (mod (n)).

In other words, pick d such that de –

1 can be evenly divided by (p-1)(q-1), the totient, or (n).

This is often computed using the Extended Euclidean Algorithm, since e and (n) are relatively prime and d is to be the modular multiplicative inverse of e.

d is kept as the private key exponent. The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption

I. Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.

II. When Person B wishes to send the message ”M” to Person A, he first converts M to an integer such that 0 ¡ m ¡ n by using agreed upon reversible protocol known as a padding scheme.

III. Person B computes, with Person A’s public key information, the cipher text corresponding to c me (mod n).

IV. Person B now sends message ”M” in cipher text, or c, to Person A.

3. Decryption

I. Person A recovers m from c by using his/her private key exponent, d, by the computation m cd (mod n).

II. Given m, Person A can recover the original message ”M” by reversing the padding scheme. This procedure works since.

6. RESULT ANALYSIS

The performance of this scheme with respect to three entities: the private key generator (PKG) for increased security, the data sharer (user), and the service provider (data center). In the experiments, the programs for three entities are implemented using the public cryptographic library MIRACL programmed in C++. All experiments were repeated 100 times to obtain average results shown in this paper, and all experiments were conducted for the cases of —N— = 1024 bits and —N— =2048 bits respectively. The average time for the PKG to setup the system , where the test bed for the PKG is a DELL T5500 workstation equipped with2.13GHz Intel Xeon Dual-coredual-process or with 12GB RAM and running Windows 7Professional 64-bit operating system. It took 151 ms and 2198 ms for the PKG to setup the whole system for —N— = 1024 bits and —N— = 2048 bits respectively.

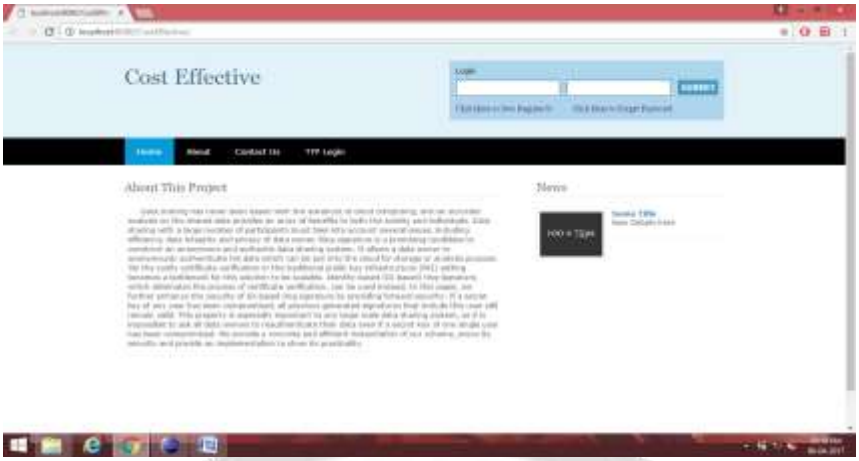

Fig -4: Home page Screenshot.

Fig -5: After login Screenshot.

7. CONCLUSIONS

Now a days security of data or information is main issues in each and every field. There is need of security and prevention of data from intrusion and misuse. We have proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. This scheme provides unconditional anonymity and can be proven forward secure unforgivable in the random oracle model assuming AES problem is hard. It is the first in the literature to have this feature for ring signature in ID-based setting. This scheme provides unconditional anonymity and can be proven forward secure unforgivable in the random oracle model assuming AES problem is hard.

8. ACKNOWLEDGEMENT

We would like to take this opportunity to express my sincere gratitude to my Project Guide Dr. M. A. Jawale (Associate Professor, IT Engineering Department) for her encouragement, guidance, and insight throughout the research and in the preparation of this dissertation. She truly exemplifies the merit of technical excellence and academic wisdom.

9. REFERENCES

[1] A. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings", CoRR, vol. abs/cs/ 0504097, 2005.

[2] P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong, "A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity (extended abstract)", in Proc. 4th Int. Conf. Provable Security, 2010, vol. 6402, pp. 166183.

[3] M. Bellare, D. Micciancio and B. Warinschi, "Foundations of group signatures: Formal denitions, simplied requirements and a construction based on general assumptions", in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003, vol. 2656

[4] A. Boldyreva, "Efficient threshold signature, multi signature and blind signature schemes based on the gap Diffe-Hellman group signature scheme", in Proc. 6th Int. Workshop Theory Practice Public Key Cryptography: Public Key Cryptography, 2003,vol.567.