

Data Integrity In Cloud Environment With Id Based Ring Signature Authentication

J.Vinodini¹, A.Prena Rashmi², Mrs.S.Revathy³

^{1,2}B.E IV Year CSE Dept, GKM College of Engineering & Technology, Chennai, Tamilnadu, India.

³ Assistant Professor- CSE Dept, GKM College of Engineering & Technology, Chennai, Tamilnadu, India.

ABSTRACT:

Cloud computing has formed the concepts and foundation basis for tomorrow's computing and is rapidly moving towards cloud based architecture. Data sharing and integrity is important thing in cloud storage. In certain situations, clients must save their information/data such as images or text in a multi cloud. Security in the Cloud is often intangible and a little bit visible, which certain creates false sense of security and anxiety about what is actually secured and controlled. When the client stores his/her data on multi-cloud servers, the distributed storage and integrity checking is very important. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification which has been used and in this paper, we further enhance the security of ID-based ring signature with 3-DES Encryption.

Keywords: *id-based ring signature, 3-DES encryption, integrity*

1. INTRODUCTION:

In our proposed scheme we use Identity based Ring Signature Technique. It also provides the authenticity and anonymity of the users. Ring signature is an assured candidate to construct an anonymous and authentic data sharing system. It permits the data owner to secretly authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be avoided costly certificate verification in the traditional public key infrastructure setting becomes limited for this solution to be scalable. Identity-based ring signature can be used to eliminate the process of certificate verification. The security of ID-based ring signature: If a secret key of any user has been revealed, previously generated signatures that make this user still remain valid. The property is especially important to any large scale network system, as it is unachievable to ask all data owners to re-authenticate

their data even if a secret key of one single user has been revealed. Accountability and privacy issues regarding cloud are becoming a significant barrier to the wide acceptance of cloud services. There is a lot of advancement takes place in the system with respect to the internet as a major concern in its exertion in a well effective manner respectively and also provide the system in a multi-cloud domain. Many of the users are getting fascinated to this technology due to the services involved in it followed by the reduced computation and by the cost and also the reliable data transmission takes place in the system in a well efficient manner respectively.

1.1 Id based ring signature

Ring signature is a group-related signature with privacy protection on signature producer. A user can sign secretly on behalf of a group on his own interest, while group members can be totally unaware of being mandatory in the group. Any verifier can be persuaded that a message has been signed by one of the members in this group (also called as Rings), but the true identity of the signer is hidden. Ring signatures could be used for anonymous whistle blowing membership authentication for ad hoc groups and many different applications which do not want intricate group formation stage but require signer anonymity.

1.2 Triple DES

In cryptography, Triple Data Encryption algorithm is a symmetric-key block cipher, which implements the Data Encryption Standard (DES) cipher algorithm three times to each data block. Originally DES cipher's key size is 56 bits that was generally sufficient when that algorithm was designed. Triple DES provides a relatively easy method of increasing the key size of DES to protect against hacker attacks, without the need to design a completely new block cipher algorithm.

2. EXISTING SYSTEM

Cloud Computing is the result of growth in the existing technologies. Cloud Computing is profitable not only for customers/users but also for large and small organizations. The existing system is Certificate Verification Technique. The weaknesses we uncovered mainly center around the fact that the cloud providers we compared were each operating in a Certificate Authority sufficiency to facilitate data sharing. In this capacity, they consider the role of both certificate issuer and certificate authorizer as denoted in a Public-Key Infrastructure (PKI) scheme - which provides them the ability to view user data inconsistency their claims of 100% data confidentiality. But it is costly verification technique but it provides strong security mechanism. Yet the costly certificate verification in a traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. The main concept of Existing system is that for each data sharing mechanism, there are integral weaknesses that can expose user all data to the cloud provider which directly contradicts the aforementioned CSP claims.

2.1 Public Key Infrastructure Scheme

The Public Key Infrastructure in cryptography is an arrangement that binds keys with respective identities of entities (like persons and organizations). The binding is established through a process of registration and issuance of certificates at and by certificate authority (CA). The PKI role that assures valid and correct registration is called registration authority (RA). An RA is responsible for accepting requests for digital certificates and authenticating the entity making the request.

2.2 Disadvantages

1. When a key is known to be compromised it could be fixed by revoking the certificate, but such a compromise is not easily noticeable and can be a huge security breach.
2. It is time consuming as Data owner should be always available for validation process
3. The issuing of certificate for every user verification is costly one.
4. Lengthy Process.

3. MODULE DESCRIPTION FOR PROPOSED SYSTEM

3.1 Cloud Service Provider

In this paper we have introduced the Cloud Service Provider (CSP), in which Data Owner registers with their Username and Password in Cloud by Cloud Service Provider for uploading data. It reduces the work load of Data Owner. The cloud provider has to make sure that it has a well-designed management infrastructure so that all of its services operate efficiently and safely. The cloud service provider has to manage both virtual as well as physical components.

3.2 Our Proposed 3DES Encryption with ID based ring signature.

The Triple DES actually uses a “key bunch” method that consists of three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

The encryption technique is as follows:

Cipher text = EK3 [DK2 [EK1 [plaintext]]]

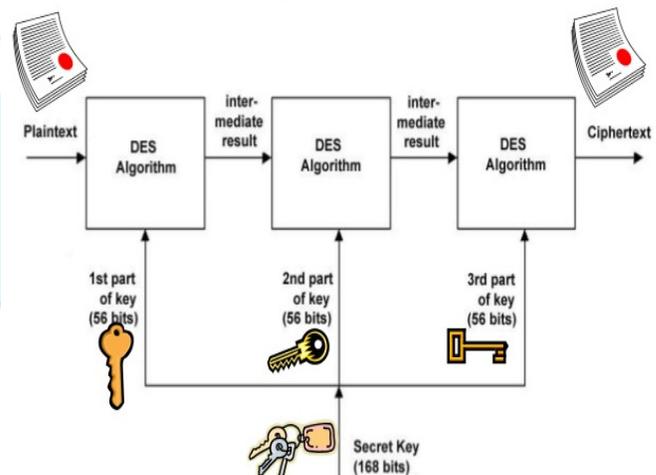
I.e., DES encrypts with K1, DES decrypts with K2 and then DES encrypts with K3.

Decryption is the reverse:

Plaintext = DK1 [EK2 [DK3 [cipher text]]]

I.e., decrypts with K3 and encrypts with K2, then decrypt with K1. Each triple encryption algorithm encrypts one block of 64 bits of data. In each case the centermost operation is the reverse of the first and last. This improves the strength of the method when using keying option 2, and provides backward congruity with DES with keying option 3.

Triple DES



3.3 Validation

The next process will be of user Registration by providing their Username and Password with Cloud Service Provider to Access Data Resources that are available on Cloud. After Successfully Uploading Data on Cloud, User Sends Request to Cloud Service Provider to access Data.

4. SYSTEM ARCHITECTURE

In our proposed scheme we use the Cloud Service Provider instead of Data owner directly. Previously if a user wants to access data it has to rely on Data owner. The data owner should be available to user all the time, it would be impossible and it will lead user to wait for availability of data owner.

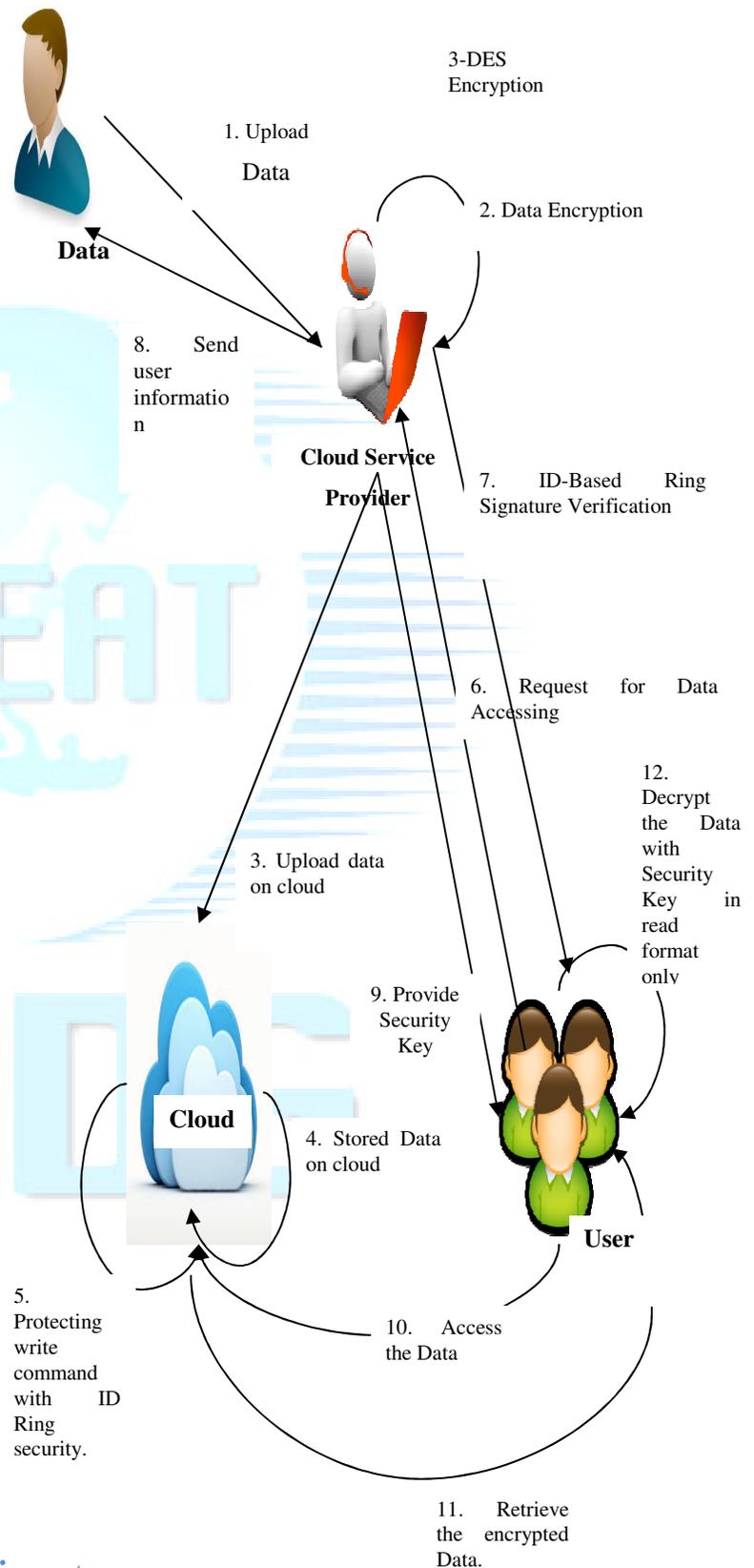
So to overcome this CSP has been introduced, it will perform all the function of the data owner. First data owner uploads its data to CSP then cloud service provider performs encryption on uploaded data. The encryption technique used is Triple Data Encryption Standard (3DES).

The CSP uploads the encrypted data to cloud. In cloud stored data is been protected using the right command with ID based ring security. Now the user does not need to rely on data owner availability it can request to access data to CSP. The CSP then provides one secret security key to both data owner and user. Through using Id based ring signature CSP validates the user authentication.

The user after getting secret key request cloud for stored data. Using the secret key only the user can decrypt the data and use it. But the data will be in the non editable format i.e., user cannot modify the document can only read.

4.1 Advantages

1. The proposed technique is cheaper than existing technique.
2. The requested data is being accessed directly through CSP so it consumes less time.
3. The data is being in a read only format so others cannot modify the data, its posse's high security.
4. Easy to access the data on cloud.



5. CONCLUSION

In this paper we have used encryption technique for secure data sharing between Data owner and user. Also we have used Cloud Service Provider to reduce the work load of Data owner which uses the ID based ring signature for authentication. The CSP provides one secret key to each user whenever user request to access the data. The data which user receives will be in a non editable format which enhances the security of Data leakage.

6. ACKNOWLEDGMENT

We would like to thank IJREAT for giving such wonderful platform for the UG students to publish their paper. Also would like to thank our Professor Mrs.R.Revathy for her constant motivation and support for us. Our sincere thanks to GKM COLLEGE OF ENGINEERING AND TECHNOLOGY, CHENNAI for proving us strong platform to develop our skills and confidence.

7. REFERENCES

- [1] M.Abe, M.Ohkubo, and K.Suzuki. 1-out-of-n Identification from a Variety of Keys. In ASIACRYPT 2002, volume 2501 of Lecture Note in Computer Science, pages from 415–432. Springer, 2002.
- [2] R. Anderson. Two remarks on public-key cryptology. Manuscript, Sep. 2000. Related material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.
- [3] A. K. Awasthi and S. Lal. Id-based ring signature and proxy ring signature scheme from bilinear pairings. CoRR, abs/cs/0504097, 2005.

