# Review on Forward Secure Identity based Ring Signature for Data Sharing in the Cloud

Priti Rumao
M. Tech Student
Computer Science and Technology
Usha Mittal Institute of Technology
SNDT University

Sumedh Pundkar
Assistant Professor
Computer Science and Technology
Usha Mittal Institute of Technology
SNDT University

## ABSTRACT
The key feature of cloud computing is one can access information any place, anywhere, at any time. So basically cloud computing is subscription based service where one can obtain network storage space and computer resources for data storage as well as data sharing. Due to high fame of cloud for data storage and sharing, large number of participants gets attracted to it but it leads to issue related to efficiency, Data integrity, privacy and authentication. To overcome these issues, concept of ring signature has been introduced for data sharing amongst large number of users. Ring signatures are used to provide user's anonymity and signer's privacy. Use of ID-based ring signature, removes the need of certificate verification which was done using public key infrastructure, hence reduce cost as well as introduction of forward security, further strengthen this system more. Use of weil pairing, keeps even shorter keys secure and it also requires less processing power. So the motivation of this paper is to propose a secure data reading and sharing scheme using above mentioned scheme.

## Keywords
Authentication, data sharing, ring signature, forward security, cloud computing.

## 1. INTRODUCTION
Cloud computing or internet-based computing provides different services such as servers, storage and applications, which via internet are delivered to an organization's devices. The characteristics of cloud such as third party, on-demand, self-service, pay-per-use and seamlessly scalable computing resources and services helps in reducing capital as well as operational costs for hardware, networking and software. These characteristics give fame to cloud computing for data reading and sharing in extensive manner amongst participants. With the advantages of cloud, data sharing with others provide number of benefits to people and society. But with increasing number of participants, it is difficult to maintain key features of data sharing such as data efficiency, integrity and privacy. To overcome these issues, concept of ring signature has been introduced for data sharing. The concept of ring signature was introduced by Rivest, Shamir and Tauman in [7]. The ring signature allows a user from a set of possible signers, to convince the verifier that the author of the signature belongs to the set of group of authenticated signers but identity of the author is not disclosed. It allows a data owner for analysis purpose as well as data storage on cloud by secretly authenticate his data using ring signature concept. The concept of ring signature can be understood as a simplified group signature which consists of only users, without the leader. It guards the anonymity of a signer because the verifier knows only that the signature belongs to a member of a ring, but doesn't know exactly who the signer is. There is no way to revoke the anonymity of the signer from ring. Unlike the group signature schemes, the ring signature scheme requires no group manager, or a setup procedure, or the action of non-signing members. For signing any message m, the signer may choose random set of other possible signers including him, to produce a valid ring signature. Introduction of forward security to the ring signature effectively enhances its safety feature.

The forward security allows a user to register with system with any public key. User safe keep his corresponding private key. The time during which the public key will remain valid, say T, will be divided into smaller time slots, like, 1,…,T. Public key stays fix throughout this time span T, whereas in each time slot user evolves secret key using different signature mechanism for each time slot. Hence even if one key from certain time slot has been exposed then to, it is difficult to find out previous or next keys. For user changing the exposed key is also an easy mechanism.

For signature generation, the concept of weil pairing over elliptic curve cryptography will be used. It is based on pairing on elliptic curve functions over finite fields. With weil pairing ECC is the strongest asymmetrical encryption method which requires less processing power and hence will work on reducing execution time parameter [8].

In order to construct the cost-effective authentic and anonymous data sharing system, forward secure ID-based ring signature with weil pairing is an essential tool. Forward secure identity based ring signature with weil pairing for data sharing in the cloud provide secure data sharing within the group in an efficient manner.

## 2. RELATED WORK
### 2.1 Identity based Ring Signature:
Javier Harrange IIIA, "Identity- Based Ring signature from RSA".

Identity-based cryptosystem excludes the need for validity checking of the certificates and a need of registering of certificates before getting the public key. These two features are suitable for ring signature where, user (signer) can anonymously sign a message on behalf of entire group with the group authenticate signature. Here the identity based ring signature and distributed ring signature involves use of many public keys. It is fascinating to consider an id-based construction which avoids the use of many digital certificates hence eliminating cost. The permanent property of id-based ring signature scenario is, formally presented and analyzed as:

Opening the anonymity of a signer (signature) is possible when the authenticate author (manager) wants to do it. Here the security of schemes can be proved using oracle model.

Basically it is designed to shape-up culled messages/identities attack [2].

**Advantages:**

- Ring structure formation for data sharing.
- Eliminates the certificate verification cost.

## 2.2 Non-Pairing ID-based threshold ring signature scheme

P.P.Tsang et.al., "A suite of Non pairing id based threshold Ring signature Schemes with Different levels of Anonymity."

Here the public key of each user can be easily identified. A private key generator (PKG) and signer then compute private keys from it. This public-private key property avoids need of digital certificate validation [3].

**Advantages:**

- Eliminate certificate validation cost.
- Secure and easy key generation.

## 2.3 Forward Secure Digital Signature Scheme

Mihir Bellare and Saro k. Miner, "A Forward-Secure Digital Signature Scheme".

Here, public key is adjusted but secret signing key is updated at conventional intervals to provide forward security property as: compromise of current secrete key does not enable any opponent to forge signature modified in the past. This controls damage cause by key exposure without requiring distributions of keys. The construction is done based on signature scheme and arbitrary oracle model proved the forward security based on the hardness of factoring [4].

**Advantages:**

- Even after secure key are exposed past signatures remain secure.

## 2.4 Security and Privacy-Enhancing multi cloud Architecture

Jen-Matlhians Bohli, Nils Gruschka, Meiko Jenson, **"**Security and Privacy-Enhancing multi cloud Architecture"

Adaptation of cloud for data sharing and storage still faces security challenges. When data is stored an multiple clouds, its integrity is checked by receiving multiple results from one operation which is performed on different cloud and compare them within own premise. This allows checking integrity of results. In applications logic is fragmented to distinct clouds. It has two benefits.

First –No cloud provider will know the entire logic.

Second – No cloud provider will learn entire calculated result of applications and hence maintains application confidentiality [5].

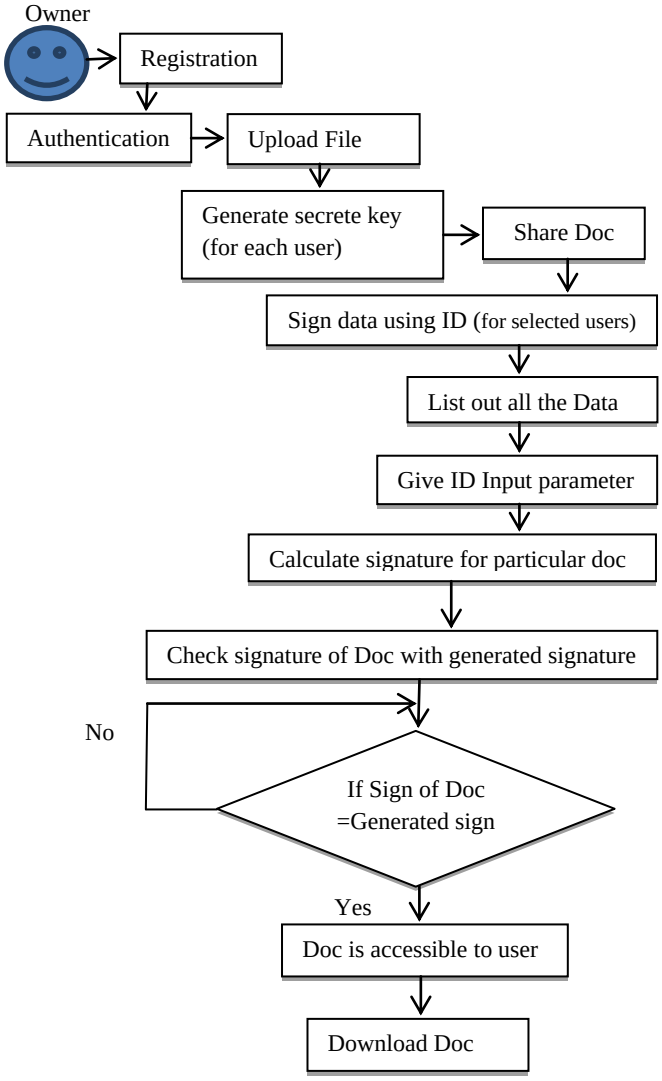
**Advantages:**

- Supports data sharing in multi cloud environment.
- Provide data security in multi cloud.

# 3 PROPOSE SYSTEM

The combined advantages of two techniques i.e the ID Based crypto system and ring signature as well as weil pairing has been used in proposed system. In this scheme the data or information should be shared across different location. Weil Pairing Signature is an essential tool for building cost-effective authentic and anonymous data sharing system. The basic process will be: User will be registered end authenticated into the system. Once it is done then system will generate secret key for each user. Owner (user) will upload the document to the System. The user who wants to share a doc (selected users), has to sign this data by using ID-based Signature (For selected users). To access particular data by some user, he has to give his ID input parameter. Based on the document information and user information, the signature for that particular doc will be calculated. Signature of that doc and the generated signature will be checked, if it is same then that doc is accessible to that user. Once the signature is verified by the system for a doc to which user is going to accesses, then that doc is available for download.

# 4 SYSTEM FLOW




# 5 SYSTEM FEATURES

**Owner Module**

In this module the owner upload the doc to the System.

**Registration Module:**

In this module, user registers into the system.

**Authentication:**

In this module, user authenticates into System.

**Generate Secret Key (for each user):**

In this module the system will generate Secret key **for each user**.

**Signing Doc for Sharing:**
In this module the user who wants to share a doc (selected users) he has to sign this data by using ID-based Signature. (For selected users)

**Verify:**
In this module we list out all the data to login user. Then to access particular data he has to give his ID input parameter then based on the document information and User information we calculate the signature for that particular doc and then we check the signature of that doc and the generated signature is same then that doc is accessible to that user.

**Data Retrieval:**
Once the signature is verified by the system for a document to which user is going to accesses then that doc is available for download.

# 6 CONCLUSION AND FUTURE SCOPE

This paper reviews various existing techniques for efficiency, data authenticity and anonymity for cloud storage. ID-based ring signature provides a sound solution on data sharing with a large number of participants. Key exposure is the fundamental limitation of ring signatures. The notion of forward secure signature was proposed to preserve the trustworthiness of past signatures even if the current signature (secret key) is compromised. Use of weil pairing will also keep small keys secure. This paper proposes a scheme which is improvement over existing techniques on basis of execution time parameter.

# 7 REFERENCES

[1] Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou "Cost-effective authentic and anonymous data sharing with forward security".DOI:10.1109/TC.2014.2315619,IEEE Transactions on Computers.

[2] Javier Herranz IIIA, "Identity-Based Ring Signatures From RSA " Artificial Intelligence Research Institute, CSIC, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain

[3] 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. 166–183.

[4] Mihir Bellare and Sara K. Miner" A Forward-Secure Digital Signature Scheme" Dept. of Computer Science, &Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA.

[5] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And Privacy-Enhancing Multi cloud Architectures" Member, IEEE, Luigi Lo Iacono.

[6] Gene Itkis Boston University Computer Science Dept.111 Cumming ton St. Boston, "Forward security: Adaptive cryptography-time evolution" MA 02215, USAitkis@bu.edu

[7] Adi Shamir, R. Rivest and Y. Tauman, "How to leak secret", In Asiacrypt'01 LNCS 2248 (2001), 552-565.

[8] Aftuck, Alex Edward, "The Weil Pairing on Elliptic Curves and Its Cryptographic Applications" (2011). UNF Theses and Dissertations. Paper 139. http://digitalcommons.unf.edu/etd/139