

# Development of an Authentic and Anonymous Data Sharing Using Ring Signature

N. Ravali & Dr. T. Sunil Kumar  
<sup>1</sup>PG Student, <sup>2</sup>Associate Professor

Vnr Vignana Jyothi Institute of Engineering and Technology, Telangana, Hyderabad.

## Abstract

*Data sharing with a huge number of participants consider many concerns, together with efficiency, data integrity and privacy of data owner. Data sharing became tedious with the cloud computing that can be addressed by the precise analysis on the shared data. It will make accessible a range of profits to both the society. Ring signature provides authentication to user data that can be placed in to the cloud for storage or scrutiny purpose. In this technique costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a holdup. In Identity-based (ID-based) ring signature, process of certificate verification is eliminated. In this paper, the security is improved by forward security. In this process any user a secret key will be compromised.*

Keywords: - Public key infrastructure, Ring signature, data integrity.

## 1. INTRODUCTION

The popularity and widespread use of “CLOUD COMPUTING” made sharing of data with others users to a number of profit to the public. Due to its ingenuousness, data sharing is always deployed in an aggressive environment and exposed to a number of security threats. The security goals in Smart Grid are as follows

**Data Authenticity:** In Smart Grid, the statistic energy usage data would be misleading if it is copied by adversary. This problem can be solved by cryptographic tools.

**Obscurity:** Energy usage data contain enormous information of consumers, from which one can haul out the number of persons in the home of consumers in such applications, and any failures may lead inconvenience to go halves data with others.

**Efficiency:** The number of users in a data sharing system could be HUGE a smart grid with a country size may practically reduce the system efficiency.

## 2. METHODOLOGY

Ring signature constructs a secret and genuine data sharing system. After data owner authentication only data will kept in to the cloud for storage or analysis. The proposed method

eliminates the process of certificate verification by providing forward security key process. In the process of forward security key a secret key of user will be compromised then all previous generated signatures that include this user still remain valid.

After careful analysis the system has been identified to have the following modules:

### 2.1 Authentication

Identity will be confirmed by the process of Authentication. Authentication can be verifying the person's documents, verifying the validity of a Website with a digital certificate. Carbon dating is the process of authentication to trace the age of an artifact. Finally we can say that authentication is the process of verification and validation with some proof.

### 2.2 Data distribution

Data sharing become put into be relevant of making data available for scholarly researchers and other investigators Transparency and openness are considered as the scientific method in data sharing [1].

Data sharing should protect institutions and scientists from use of data for biased purposes. By providing policies on data archiving data can be saved from corruption and loss by providing confidentiality.

### 2.3 Cloud computing

Cloud computing is the process which computes clusters of isolated servers and software networks. It allows numerous categories of data sources be uploaded to cloud for real time analysis of data.

### 2.4 Ring Signature

Shamir introduced the process of Identity-based (ID-based) cryptosystem. This process is free from the verification and validation of public key certificates.

So it reduces the time and cost consumption. When huge number of users are involved in communication PKG significantly save the communication and computation time by eliminating the certificate verification.

## 2.5 Forward security

In cryptography Forward secrecy is used for key-agreement. This protocols ensures the session key consequential from a set of long-term keys cannot be conciliation if one of the long-term keys is conciliation in the future. The revelation of one user's secret key turn into all previously obtained ring signatures in to invalid state.

### 1. Smart grid

Smart grid gathers the information and analyses like information about the behaviors of suppliers and consumers. This analysis on data will be in a mechanized method to improve the effectiveness trustworthiness, economics, and sustainability of the system.

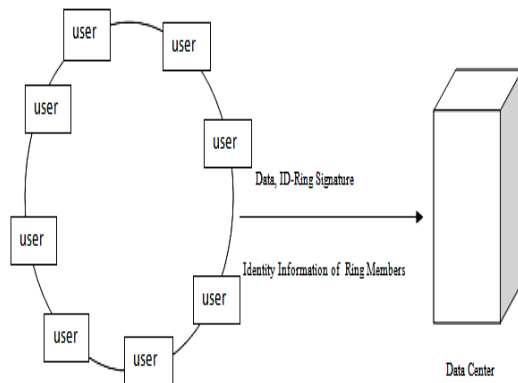


Figure 2.1 Proposed systems for Ring Signature Ring signature based proposed system is shown in Figure2.1.

- Step 1: In first phase needs public characteristics ring members, such as residential addresses etc.
- Step 2: user identify information of the ring members by uploading their personal data of electronic usage.
- Step 3: The verification of ring signature provides data authenticity to data provider

## 3. IMPLEMENTATION

For the experimentation, the programs are written in C++. All experiments were conducted for different the cases.1024 bits and 2048 bits respectively. After careful analysis the system has been identified to have the following modules:

**Data Owner** The data owner is liable for collect documents, and distribution of encrypted format to the cloud server.

**Date User** whenever data user wants to access the data should be authorized from the data owner.

**Cloud Server** This server is semi-trusted , will contain enormous stowage capacity and the working out resources required for the cryptography. Whenever cloud gets the request from the user, upon searching the encrypted index it responds with the top-k documents which will be near match to the users query or request. K is the choice of the data user. This proposed system protects data from cloud server without disclosing the information to it in the way of improving the efficiency of cipher text search.

## 4. EXPERMENTAL RESULTS

In this section analysis on the results obtained for the proposed system is discussed. As the part of the system user should register as the data owner to generate private key as shown in the Figure4.1.

Figure4.1 User login after registration

Figure4.2 Creating Ring groups

The group id of the user is used to join in the group as shown in the

Figure4.2.

Userid	Username	GroupName	Group Id	Accepted
8	ravali	localgroup1	10	ACCEPT

Figure4.3a Group id accept in the group

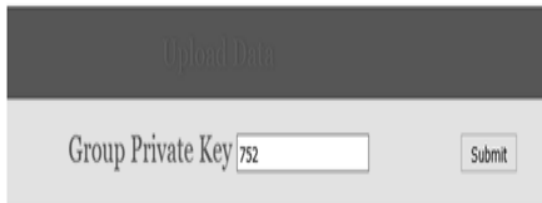


Figure4.3b obtaining group private key  
To communicate in the group acceptance is required, once recognized in the group private key will be assigned as shown in Figure 4.3a, 4.3b.


UserDetails				
Userid	FirstName	Username	Emailid	Photos
5	a	a	a@gmail.com	
6	santanu	santanu	santanu.asc@gmail.com	
7	raja	raja	santanu.acr@gmail.com	
8	ravali	ravali	ravali.1502@gmail.com	

Figure4.4 Display of user-id in the group  
The complete details of users in the group are displayed in the Figure4.4.

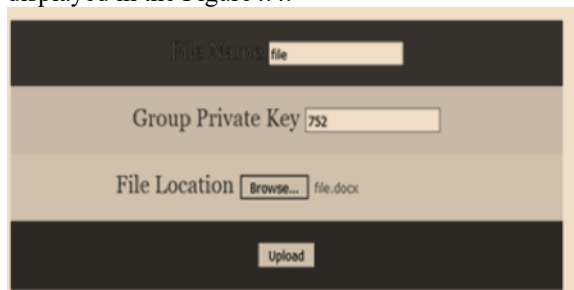


Figure4.5a Authentication for file access

Fid	Userid	GroupKey	FileName	Accepted
8	file	752	file	Check Now

Figure4.5b Permission for file access  
To access the file in the group authentication will be performed by verifying the group private key as shown in Figure 4.5a, 4.5b.

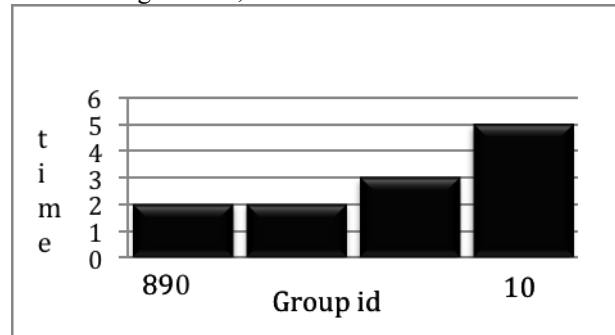


Figure4.6 Performane graph  
As the users in the group increases the time required for access will increases shown in Figure4.6.

## 5.SUMMARY

In this paper, cipher text is used to search in the cloud storage. The experiment improves in search efficiency rank security by increasing the relevance between retrieved documents.

The proposed system provide forward security. It provides unconditional nonymity. This scheme will not necessitate any coupling operations. The size of user secret key is just one integer.This scheme will be used in smart grid applications.

## References

- [1].Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.Katz,A.Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, andM. Zaharia, "A View of Cloud Computing," Commun. ACM,vol. 53, no. 4, pp. 49-58, Apr. 2010.
- [2] H. Biggar, "Experiencing Data De-Duplication: Improving Efficiency and Reducing Capacity



Requirements,” Enterprise Strategy Grp., Milford, MA, USA, White Paper, Feb. 2007.

[3] C.Liu,Y.Lu,C.Shi,G.Lu,D.Du,andD.-S.Wang,“ADMAD:Application-Driven Metadata Aware De-Deduplication Archival Storage Systems,” in Proc. 5th IEEE Int’l Workshop SNAPI I/Os,2008, pp. 29-35.

[4] A. Katiyar and J. Weissman, “ViDeDup: An Application-AwareFramework for Video De-Duplication,” in Proc. 3rd USENIXWorkshop Hot-Storage File Syst., 2011, pp. 31-35.

[5]Y.Tan,H.Jiang,D.Feng,L.Tian,Z.Yan,andG.Zhou,“SAM:A Semantic-Aware Multi-Tiered Source De-Duplication FrameWorkfor Cloud Backup,” in Proc. 39th ICPP, 2010, pp. 614-623.

[6] A. Muthitacharoen, B. Chen, and D. Mazieres, “A LowBandwidth Network File System,” in Proc. 18th ACM SOSP,2001, pp. 174-187.

[7] S. Kannan, A. Gavrilovska, and K. Schwan, “Cloud4HomeVEnhancing Data Services with @Home Clouds,” in Proc. 31<sup>st</sup> ICDCS, 2011, pp. 539-548.

[8] Maximizing Data Efficiency: Benefits of Global DeduplicationNEC,Irving, TX, USA, NEC White Paper, 2009.

[9] D. Meister and A. Brinkmann, “Multi-Level Comparison of Data Deduplication in a Backup Scenario,” in Proc.2ndAnnu.Int’l SYSTOR, 2009, pp. 1-8.

[10] D. Bhagwat, K. Eshghi, D.D. Long, and M. Lillibridge, “Extreme Binning: Scalable, Parallel Deduplication for Chunk Based FileBackup,” HP Lab., Palo Alto, CA, USA, Tech. Rep. HPL-200910R2,Sept. 2009.

[11] B. Zhu, K. Li, and H. Patterson, “Avoiding the Disk Bottleneck in the Data Domain duplication File System,” in Proc. 6<sup>th</sup> USENIX Conf. FAST, Feb. 2008, pp. 269-282.

[12] M. Lillibridge, K. Eshghi, D. Bhagwat, V. Deolalikar, G. Trezise, and P. Camble, “Sparse Indexing: Large Scale, Inline Deduplication Using Sampling and Locality,” in Proc. 7th USENIX Conf. FAST, 2009, pp. 111-123.

[13] P. Anderson and L. Zhang, “Fast and Secure Laptop Backups With Encrypted De-Duplication,” in Proc. 24th Int’l Conf. LISA,2010, pp. 29-40.