International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Improving Security Level of Id Based Ring Signature Using Forward Security

Sachin Kharade[1], Amit Dangy[2]

[1]*Pursuing M.Tech, CSE Branch, Dept of CSE, Institute of Technology and Management , Bhopal, M.P., India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Institute of Technology and Management , Bhopal, M.P., India*

***Abstract*-- Sharing of Information in a cloud environment is inevitable in onward of cloud computing environment. Data sharing has never been easy with the advancement of cloud computing. The correct study on the shared data provides number of benefits to both the society and individuals. Storage-as-a-service obtainable by cloud service providers (CSPs) is paid ability that enables organizations to delegate their sensitive data to be stored on inaccessible servers. Getting Certificate and for every access is long process and cost increases. In Identity-Based (ID Based) Ring Signature Members of this group can easily share data avoiding the pricey certificate verification as done in the usual procedure. Forward Security re authentication overhead is avoided in Ring Signature by using RSA Algorithm we further provide increased level of security in reduced time, efficient and simple manner. This paper proposes a cloud based storage method that allows the data proprietor to benefit from the convenien ces offered by the CSP and enables trust between them. Identity-bas- ed (ID-based) ring signature, which removes process of certificate verification, can be used as a alternate. In this paper, we proposed the security of ID-based ring signature by providing forward safety: If a top secret key of any user has been compromised, all preceding generated signatures that include this user still longer valid. This pro-perty is specially important to any large scale data distribution system, as it is not possible to ask all data owners to again authenticate their data even if a secret key of any user has been compromised. It allows the proprietor to funding or revoke admittance to the outsourced data.**

***Keywords*—cloud computing, forward security, smart grid, data distribution, Authentication**

I. INTRODUCTION

The popularity and widespread use of “CLOUD" have brought great convenience for data sharing and collection can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society as well. As a representative example,consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm (Fig. 1). From the collected data a statistical report is created, and one can compare their energy consumption with others (e.g., from the same block). This ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage. Due to its openness, data sharing is always deployed in a hostile environment and vulnerable to a number of security threats. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, including:

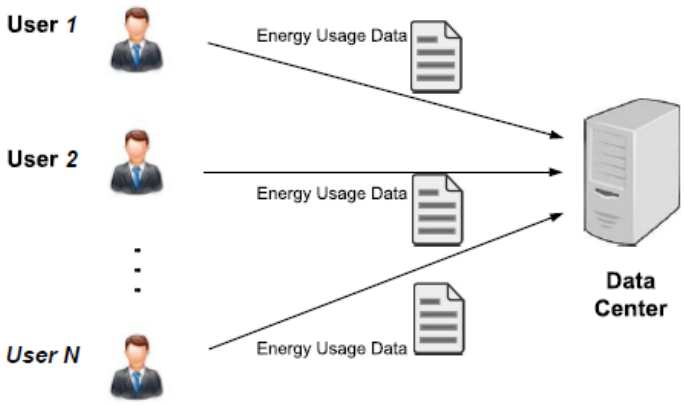

Figure 1: Energy Usage Data Sharing in Smart Grid

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

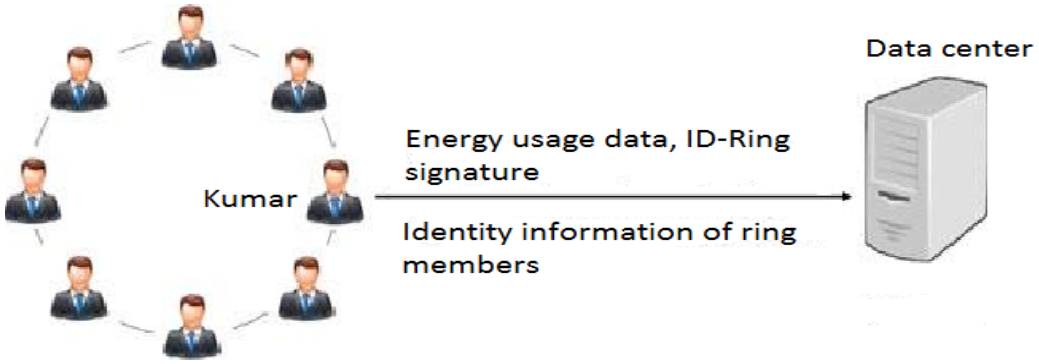

Figure 2: A solution based on ID-based ring signature.

- *Anonymity:* Energy usage data contains vast information of consumers, from which one can citation the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such applications, and any failures to do so may lead to the reluctance from the consumers to share data with others.
- *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. Otherwise it would lead to a waste of energy, which contradicts the goal of Smart Grid.

II. ID-Based Forward Secure Ring Signature Scheme Design

ID-based forward secure ring signature scheme are designed to following ways. The identities and user secret keys are valid into T periods and makes the time intervals public and also set the message space M= { 0,1 }*.

A. Setup

On input of a security parameter λ, the PKG generates two random k-bit prime numbers p and q such that p = 2p′ +1 and q = 2q′ +1 where p′, q′ are some primes. It computes N = p*q. For some fixed parameter it chooses a random prime number e such that and gcd (e, (N)) = 1. It chooses two hash functions H1 :{0,1}*→ ZN* andH2 : {0,1}*→{0,1}. The public parameters param are (k,l,e,N,H1,H2) and the master secret key msk is (p, q). On input of a security parameter λ, the PKG generates two random k-bit prime numbers p and q such that p = 2p′ +1 and q = 2q′ +1 where p′, q′ are some primes. It computes N = p*q. For some fixed parameter it chooses a random prime number e such that and gcd (e, (N)) = 1. It chooses two hash functions H1 :{0,1}*→ ZN* andH2 : {0,1}*→{0,1}.

The public parameters param are (k,l,e,N,H1,H2) and the master secret key msk is (p, q).

B. Extract

For user i, where i Z, with identity IDi {0,1}* requests for a secret key at time period (denoted by an integer), where 0 ≤t < T, the PKG computes the user secret key using its knowledge of the factorization of N.

$$sk_{i,t} = [H_1(ID_i)]^{\frac{1}{e^{(T+1-t)}}} \bmod N$$

C. Update

On input a secret key sk i,t for a time period t, if t < T the user updates the secret key as otherwise the algorithm outputs meaning that the secret key has expired.

D. Sign

To sign a message m {0,1}* in time period t, where 0 ≤t < T, on behalf of a ring of identities L = {ID1,….,IDn}, a user with identity ID . Land secret key sk t:

1)For all i{1,…..n},i#,choose random *Ri=Ai e(x+1-t) mod N and hi = H2(L,m,t.ID, Ri)*

2) choose random A Z*N and compute

$$R_\pi = A_\pi^{e^{(T+1-t)}} \cdot \prod_{i=1, i\neq\pi}^{n} H_1(ID_i)^{-h_i} \bmod N$$

3) Compute s= (sk t)h *Πni=1 Ai mod N*

4) Output the signature for the list of identities L, the message m, and the time period t as = (R1,…..,Rn,h1,….,hn,s)

E. Verify

To verify a signature for a message m, a list tf identities L and the time period t, check whether hi = H2 (L,m,t,IDi,Ri) for i=1,…, n and

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

$$s^{e^{(T+1-t)}} = \prod_{i=1}^{n} \left(R_i \cdot H_1(ID_i)^{h_i} \right) \bmod N$$

Output valid if all equalities hold otherwise output invalid.

Projected scheme involves the exponent e larger than 2, where 'e' is the bit length of the hash function H2. Frequently a secure hash function requires at least 160 bits output. However, if we set 160 it will be quite inefficient. In order to offset this, we can use different hash functions such that each hash function outputs '0 bits.

We are supposed to reiterate the signing and verification procedures 8 times for each time using a different hash function H2 in order to achieve 160-bit hash function security. The size of public parameters is a constant, which only consists of some security parameters, two integers and some hash functions. The secret key is very short and only an integer. Let us assume to use 1,024-bit RSA security level, the secret key is just 1,024 bits. For every key update process, it just requires an exponentiation with exponent e over modulus N operation. The signing and verification algorithms do not require any pairing operation. The computation complexity and space requirement of this scheme are shown in below table respectively.

Table 1:
No. of user and their time

No of Users in Ring	Reduced Timing When Security is Incresed		
	T=100	T=200	T=300
N=10	500	600	700
N=20	650	700	500
N=30	700	600	650
N=40	800	600	850

(Unit: ms)
Parameters: |N|=1024,|K|=512 (a)

III. Implementation And Experimental Results

For the proposed system performance evaluation, we calculate matrices for accuracy. We implement the system on java 3-tier MVC architecture framework with INTEL 1.70 GHz i3 processor and 4 GB RAM.

Here each graph shows the system performance with different experiments that has been classified in graphs.Here in graphs, X axis shows the total number of user and Y shows the time required in milliseconds for performing such operation T is the transactions.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

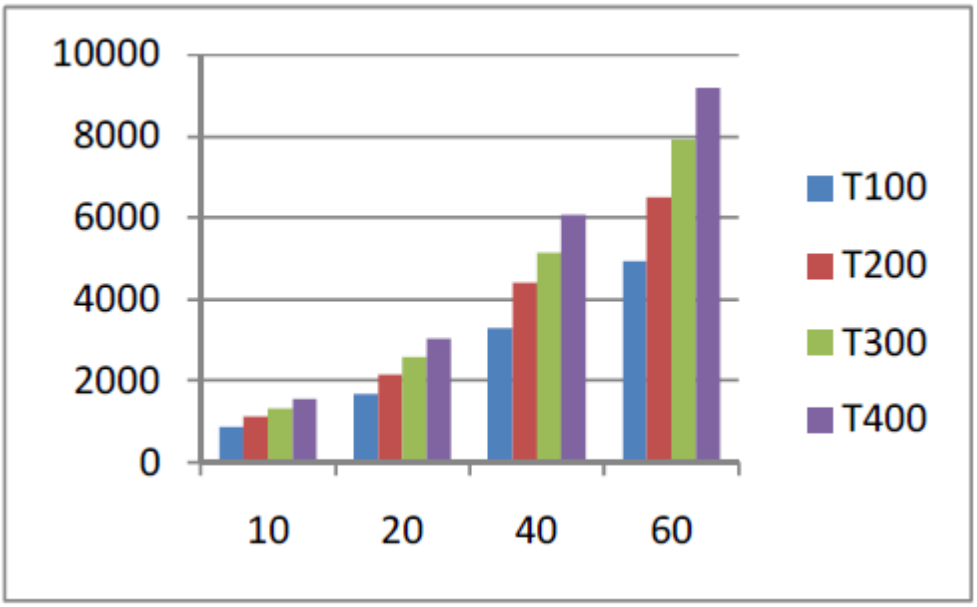

Figure 1: The average time for the data owner to create signature, when key size 512 bit

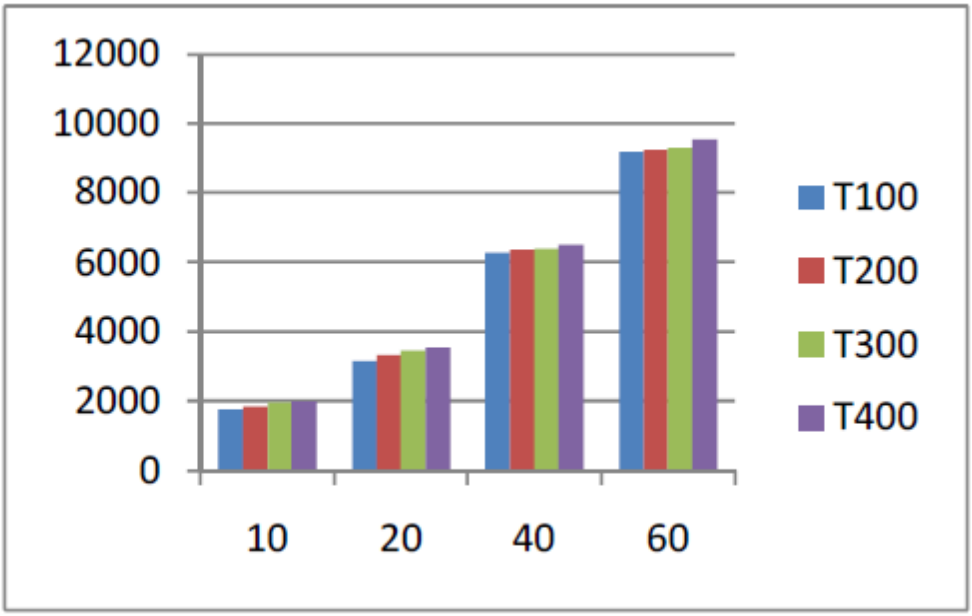

Figure 2 The average time for the service provider to verify the ring signature

Practically In this application the analysis shows the No of users and their required time for the Ring Signature.

And with that Analysis Total time is been calculated to show the analysis of no of users where register. This total time also gets saved in the database with the no of users registered in the application for ring chart.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

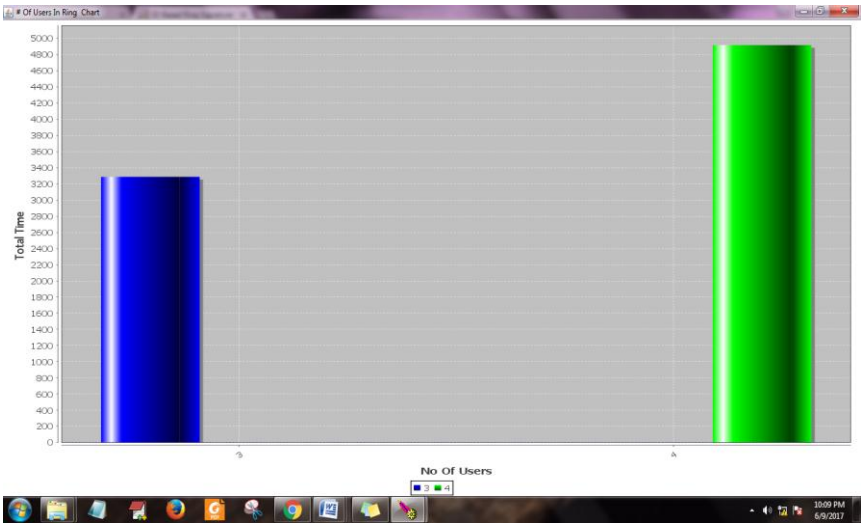

Figure 4: Ring Generation time chart

IV. Conclusion

The Forward Secure ID-based Ring Signature supports an ID-based ring plan to prove forward security. For this plan any matching operation is not required. The period of mystery key is only one whole number, while the key upgrade handle just requires an exponentiation. This will be remendously utilized in many applications, particularly to those need more security, for example, e-business exercises, e-contract signing and e-auction. The framework with multi-cloud framework improves the effectiveness, sizably voluminous capacity and information sharing framework. For this experiment, it requires less space and less time. This property minimizes the cost factor.

REFERENCES

[1] Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security" IEEE TRANSACTIONS ON COMPUTERS VOL: 64 NO: 6 YEAR 2015

[2] IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013 "Attribute-Based Access to Scalable Media inCloud-Assisted Content Sharing Networks by theYongdong Wu, Zhuo Wei, and Robert H. Deng.

[3] University of the Wollongong Research Online "Improvements on an authentication scheme for vehicular sensor networks" Liu, J. K., Yuen, T. Hon., Au, M. & Susilo, W. (2014).

[4] Liu, J. K., Au, M., Huang, X., Susilo, W., Zhou, J. & Yu, Y. (2014). New insight to a preserve online survey accuracy and privacy in bigdata era. Lecture Notes in Computer Science, 8713 (PART 2), 182-199.

[5] International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012"Distributed Accountability for Data Sharing in Cloud.

[6] IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 7, NO. 3, JULY-SEPTEMBER 2014"ASocial Compute Cloud: Allocating and the SharingInfrastructure Resources via Social Networks.

[7] IJSTE - International Journal of Science Technology & Engineering "Forward Secure Identity Based Signature for Data Sharing in the Cloud by Bindumal V.S ,Dr.Varghese Paul,Shyni S.T.

[8] IOSR Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 69-72 "PRIVACY & DATA INTEGRITY FOR THE SECURE CLOUD STORAGE.

[9] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.