ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Implementation of Forward Security System for Data Sharing With Authenticity and Cost Effective

Mihir Mohapatra[1], Prof. N.P. Karlekar[2]

Department of Computer engineering, Sinhgad Institute of Technology, Lonavala, Savitribai Phule Pune University, India.

ABSTRACT - As in today's modern world of computing where data storage is critical issue, most of the applications are getting shifted on cloud computing platform. We are habituated and getting focused on cloud environment in a large scale in these modern days. But on cloud computing data sharing is never been easier, and everyone wants that data shared should give accurate analysis which will benefit the society and an individuals.
There are large numbers of participants in data sharing and everyone need to take care of several issues like including efficiency, data integrity and privacy of data owner. Ring signature is a one such mechanism which will construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose.

But major problem with this Ring Signature is that the certificate verification for security is a costlier affair which makes the system more scalable and secure.

To avoid this bottleneck Identity-based Ring Signature which eliminates the process of certificate verification is proposed to solve this problem with further enhancement of security of ID- Based ring signature.

General Terms- The title of our paper is basically focusing on the general terms of forward security of ring based network ID system on cloud platform. We will be implementing algorithm which will assign a forward security to network.

KEYWORDS- Forward Security, Cost Effectives, Data Sharing, Cloud Computing

I. INTRODUCTION

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck forthis solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as 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. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. REVIEW OF LITERATURE

We had conducted various literature survey and some of them which are relevant to our paper are listed below.

1. Identity-based Ring Signature:
Javier Herranz IIIA, "Identity-Based Ring Signatures from RSA" Artificial Intelligence Research Institute, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain Identity-predicated crypt-systems eliminate the desideratum for validity checking of the certificates and the desideratum for registering for a certificate a for getting the public key. These two features are desirable especially for the efficiency and the authentic spontaneity of the ring signature, where a utilizer can anonymously sign a message on behalf of a group of spontaneously conscripted users including of the authentic signer. The identity-predicated ring signature and distributed ring signature schemes, involve many public keys, it is especially intriguing to consider an identity-predicated construction which evades the management of many digital certificates. The first that is distributed

ring signature schemes for identity-predicated scenarios which do not employ bilinear pairings. A paramount property of the scheme is additionally formally presented and analyzed: opening the anonymity of a signature is possible when the authentic author wants to do so. The security of all the considered schemes can be formally proved in the desultory oracle model. The security of ID-predicated signature schemes is formalized by considering the most vigorous possible kind of attacks: culled messages/identities attacks. Ring structure formation for data sharing. Eliminate the costly certificate verification.

2. Forward-Secure Digital Signature Scheme:
MihirBellare 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 Digital signature scheme in which the public key is fine-tuned but the secret signing key is updated at customary intervals so as to provide forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be utilizable to mitigate the damage caused by key exposure without requiring distribution of keys. The construction uses conceptions from the signature schemes, and is proven to be forward secure predicated on the hardness of factoring, in the arbitrary oracle model. The construction is additionally quite efficient. Past signature remain secure even if expose the current secret key.

III. SYSTEM ARCHITECTURE & OVERVIEW

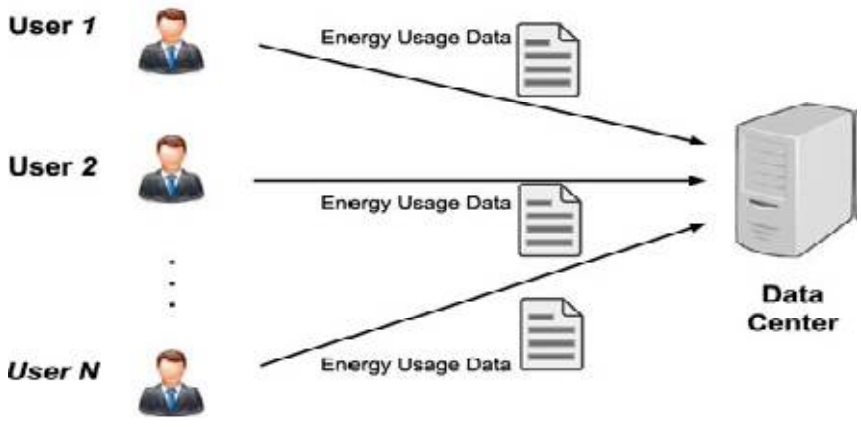

Figure 1: System Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. MATHEMATICAL MODEL

Assumption: (RSA Model):
Let N=pq, where p and q are two k-bit prime numbers such that $p=2p^1+1$ and $q=2q^1+1$ for some primes p^1; q^1. Let e be a prime[1] greater than 2^l for some fixed parameter l_1, such that
gcd(e,ϕ (^{N}))=. 1Let y be a random element in Z*N. We saythat an algorithm S solves the RSA problem if it receives aninput the tuple **(N,e,y)**and outputs an element z such that
z^e= y mod N.
Security Model:
A (1,n), ID-based forward secure ring signature (IDFSRS) scheme is a tuple of probabilistic polynomial-time (PPT) Algorithms:

- **Setup.**: On input an unary string 1^{λ} where $^{\lambda}$ is a security parameter, the algorithm outputs a master secret key msk for the third party private key generator and a list of system parameters param that includes $^{\lambda}$ and the descriptions of a user secret key space D1 a message space M well as a signature space $_{\varphi}$
- **Extract.** On input a list param of system parameters,an identity IDi€$\{0,1\}^*$ for a user and the mastersecret key msk, the algorithm outputs the user'ssecret key $sk_{i,0}$€ D such that the secret key is validfor time t = 0. In this paper, we denote time as nonnegativeintegers. When we say identity ID_i correspondsto user secret key $sk_{i,0}$ or vice versa, wemean the pair(ID_i, $sk_{i,0)}$ is an input-output pair ofExtract with respect to param and msk.
- **Update.** On input a user secret key $sk_{i,t}$ for a timeperiod t, the algorithm outputs a new user secret key$sk_{i,t+1}$ for the time period t + 1.
- **Sign.** On input a list param of system parameters, atime period t, a group size n of length polynomial in ƛ, a set L= {ID_i€ {0, 1}*|I € [1, n]} of n user identities,a message m € M, and a secret key$sk_{\pi,t}$€D,π€[1, n] for time period t, the algorithmoutputs a signature of $_{\varphi}$ **€C.**
- Verify. On input a list param of system parameters, a time period t, a group size n of length polynomial in ƛ, a set L= {ID_i € {0, 1}*|I € [1, n]} of n user identities,a message m € M, a signature € D, it outputseither valid or invalid.
- Correctness. A (1,n) IDFSRS scheme should satisfy the verification correctness—signatures signed by honest signer.

V. OUR PROPOSED ID-BASED FORWARD SECURE RING SIGNATURE SCHEME

The Design
We assume that the identities and user secret keys are valid into T periods and make the time intervals public. We also set the message space M ={0,1}*
Setup. On input of a security parameter ƛ, the PKGgenerates two random k-bit prime numbers p and qsuch that $p=2p^1+1$ and $q=2q^1+1$ where p & q are some primes. It computes N=pq. For some fixedparameter l, it chooses a random prime number esuch that $2^l < e < 2^{l+1}$ and gcd(e,ϕ (^{N}))=1. It chooses two hash functions H1 :{0,1}*→Z*N andH2 {0,1}*→$\{0,1\}^1$. The public parameters param
are {k,l,e,n,H1,H2}and the master secret key mskis (p ,q)Extract. For user i, where i € Z, with identityIDi€{0,1}, requests for a secret key at time periodt (denoted by an integer), where 0 <= t < T, the PKGComputes the user secret key

$$sk(i,t) = [H1(1,Di)]\frac{1}{e(T+1-t)} Mod\ N$$

using its knowledge of the factorization of N.Update. On input a secret key $sk_{i,t}$ for a time period t,
Ift < T the user updates the secret key ass$k_{i,t+1=(}sk_{i,t})^e$ mod NOtherwise the algorithm outputs "?" meaning thatthe secret key has expired
Sign. To sign a message m €{0, 1}* in time period t,Where 0<=t < T, on behalf of a ring of identitiesL ={ID1; . . . ; IDn} , a user with identity IDπ € Land secret key skπ;t:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Verify: To verify a signature s for a message m, a listof identities L and the time period t, check whetherhi = H_2(L,m, t, IDi,Ri) for i = 1; . . . ; n and $s^{e(T+1-t)}=\prod_{i=1}^{n}(Ri--(H1(IDi)hi)Mod\ N$

Output valid if all equalities hold. Otherwise outputinvalid.

VI. MODULES DESCRIPTION

Cloud Service Provider

1. This is our first module where we check the system model of cloud service provider with the user.
2. We had developed the Cloud Service Provider by which an entity is getting provided in cloud for data storage.
3. Through S-CSP data of user is getting stored of user on cloud.
4. The S-CSP has large amount of storage capacity and computing power and it is always on-line is our assumptions in this paper.

Data Owners Module

1. Data owner is a module which will get developed which will result in data storage to S-CSP of an entity.
2. Data Owner uploads the file on cloud.
3. This data can be accessed later on or downloaded by data owner.

ID-based ring signature

1. The data owner (any user) will choose the user from group of user in ring topology. During this phase one needs the public key identity information for the ring members like address, id etc and not requires collaboration from any other ring members
2. The user uploads his data on cloud through the upload mechanism along with ring signature and identity information of all the members of ring.
3. One has to verify the ring signature through which it can be assured that data is given by valid user from one of the ring member. Hence the data provider anonymity can be checked by signature along with data authenticity. And during this we don't require to do certificate verification.

Efficiency Analysis:

1. Hence through this ID Based ring signature is an optimal solution from all other solution to check the data authentic, anonymity and data sharing to a large number of other group participants.
2. The size of public parameters is aconstant which consist of security parameters. Typical example is two integers and some hash keys. The secret key is very short just 1 byte and hence less overhead during transmission of this keys.

VIII. SYSTEM DESIGN

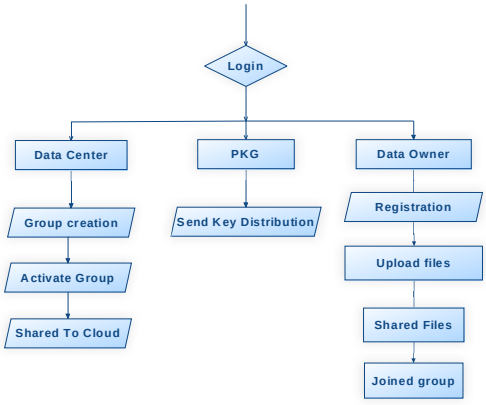

Figure 2: Data Flow of our system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

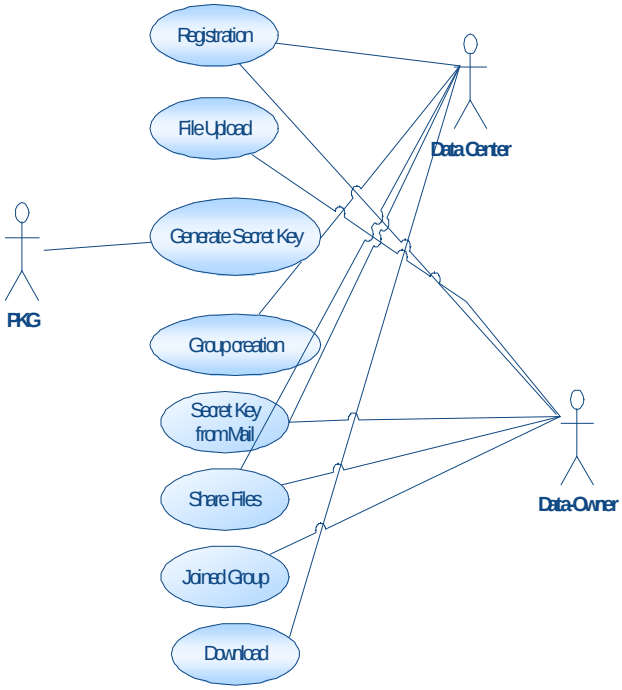

Figure 3: Use Case Diagram

IX. COMPARISON

		Solutions to key exposure problem in ring signature	Forward secure ring signature without random oracles	Our scheme
Features	Unconditional Anonymity	Yes	NO	Yes
	ID Based	No	No	Yes
	Assumption	Factorization	CDH, Subgroup Decisional	RSA
	Without ROM	No	Yes	No
Space requirement	Secret Keys(bits)	2*|N|	2*log2(T)+1*(G)	|N|
	Signature (Bits)	$n*(\|N\|+l^l)$	(2*n*+3)*(G)	$(n*(\|N\|+l)+\|N\|* l/l^l$

Notations:
ROM: Random Oracle Model;
T: number of time slots;
(H): the length of the hash of the message in binary bits;
(N): the length of N in binary bits;
(G): the length of a group element in G for elliptic curve group; (If 160 bit elliptic curve is used, (G)=160 bits.)
n: number of users in the ring;

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

‘: a fixed integer.

X. IMPLEMENTATION AND EXPERIMENTAL RESULTS

We implement the smart grid example introduced in Section 1, and evaluate the performance of our IDFSRS scheme with respect to three entities: the private key generator, the energy data owner (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 jNj ¼ 1;024 bits and jNj ¼ 2;048 bits respectively .
The average time for the PKG to setup the system isshown in Table 4, where the testbed for the PKG is a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon dual-core dual-processor with 12 GB RAM and running Windows 7 Professional 64-bit operating system. It took 151 and 2,198 ms for the PKG to setup the whole system for jNj ¼ 1;024 bits and jNj ¼ 2;048 bits respectively.

Average Time for the PKG to Setup the System

|N Bits|	Time(ms)
1024	151
2028	2198

XI. CONCLUSION & FUTURE WORK

As there is lot of need of data sharing over a cloud platform, we had proposed this ID based ring signature system which is very efficient than traditional certificate verification system.
Our Paper proposes the system which offers unconditional security and can be checked with ID based forward security. The key is just an integer value less than 1byte and it is well organized as well as does not require any pairing operation.
The key update just needs to be exponentiation. Our research will be very useful in many application where user privacy and authenticity is a prime importance like on-line banking, e commerce sites, ad hoc network to name a few. Our present scheme relies to show thesecurity. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

The average time for the data owner (user) to sign energy usage data with different choices of n and T are shown in Figs. 3 and 4, for jNj ¼ 1;024 bits and jNj ¼ 2;048 bits respectively. The testbed for the user is a laptop personalcomputer equipped with 2.10 GHz Intel CPU with 4 GB RAM and running Windows 7 operating system.The average time for the service provider (data center) to verify the ring signature with different choices of n and T are shown in Figs. 5 and 6, for jNj ¼ 1;024 bits and jNj ¼ 2;048 bits respectively. The testbed for the date centeris a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon dual-core dual-processor with 12 GB RAM and running Windows 7 Professional 64-bit operating system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

REFERENCES

[1]. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Member, IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 4, APRIL 2015.
[2]. 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.
[3]. R. Anderson, "Two remarks on public-key cryptology," Manu-script, Sep. 2000. (Relevant material presented by the author in an invited lecture at the Fourth ACM Conference on Computer and Communications Security, 1997.)
[4]. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," in Proc. 20th Annu. Int. Cryptol. Conf. Adv. Cryptol., 2000, vol. 1880, pp. 255–270.
[5]. M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, "ID-based ring signature scheme secure in the standard model," in Proc. 1st Int. Workshop Security Adv. Inform. Comput. Security, 2006, vol. 4266, pp. 1-16
[6]. A. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings," CoRR, vol. abs/cs/ 0504097, 2005.
[7]. M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions," in Proc. 22nd Int. Conf. Theory Appl.CryptographicTechn., 2003, vol. 2656, pp 614– 629