IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 06-10
www.iosrjournals.org

ID-Based Ring Signature and Anonymous Data Sharing with Forward Security

Prof.Nagare Pravin V.[1] ,Shirsath Priyanka N.[2], Rawal Sonali V.[3],
Sirsat Kanchan R.[4],Tarle Gayatri P.[5,]
[1,2,3,4,5]*(Computer, KVNNIEER, India)*

Abstract : *Due to the advance of new technology data sharing has never been easier in this world. An accurate analysis on the shared data provides a group of benefits to both the society and individuals. Data sharing between two members or group of members must take into account several issues. They are efficiency, data integrity and privacy of data owner. To overcome this issue Ring signature concept is introduced. It is a promising approach to construct a secret and authentic data sharing system which allows a owner of the data to anonymously authenticate his/her data which can be put into the cloud for storage or analysis purpose. This could be creating costly certificate verification in the traditional public key infrastructure (PKI) so this type of verification additionally create a bottleneck and scalable problem. To overcome this problem Identity-based (ID-based) ring signature could be used. The major advantage of this ID based scheme is eliminates the costly certificate verification. This paper further enhances the security by integrating ID-based ring signature with forward security. Even though a secret key of any user has been attacked or compromised, all previous generated signatures that belong to the user still remain valid. For any type of large scale data sharing system this property is especially important. It never asks data owners to re authenticate their data even if a secret key is known to the attacker. This scheme provides a concrete and efficient method.*

Keywords - Authentication , *data sharing, cloud computing, forward security, smart grid.*

I. INTRODUCTION

Ring signature allow valid user to construct a secure and effective data sharing system. By using this method an owner of the data anonymously authenticate his information which can be put into the Storage at different places along with identity information. In order to construct the cost-effective authentic and anonymous data sharing system Forward secure ID-based ring signature is an essential tool. ID-based ring signature seems to be an optimal factor which exchange among efficiency, data authenticity and anonymity. It provides a sound solution on data sharing between a large numbers of participants. One can add more users in the ring in order to obtain a higher level protection but doing this increases the opportunity of key exposure as well.

In this, the key exposure is the fundamental limitation of ordinary digital signatures. If the private key of a user is compromised and if the attacker knows partial or full key means all signatures of those users become worthless. By using this compromised signature future signatures also validated. The previously issued signatures also cannot be trusted. Once a key leakage is identified, new key generation mechanisms must be invoked immediately. By using this mechanism the generation of any password using the compromised secret key should be prevented. However, this mechanism does not solve the problem of forge ability for previously used signatures.

In order to preserve the validity of past signatures the forward secure signature was proposed this mechanism works even though current secret key is compromised. First it calculates the total time of the validity of a public key and divides them into T time periods. A key compromise of the current time slot does not enable an adversary to produce valid signatures pertaining to past time slots.

The exposure of one user's secret key may discover all previously obtained ring signatures but the condition is that user is one of the ring members. Since the member cannot identify whether a ring signature is generated prior to the key exposure or not without using any mechanism. So the forward security is a necessary requirement in a big data sharing system. Otherwise, huge amount of time and resource will be waste. The forward-secure digital signatures should be designed in various fashions in order to add forward security on ring signature. Two types forward secure ring signature schemes they are discussed in [1], [2]. However they both work in the traditional public key setting. In this type of settings the signature verification involves expensive certificate check for every ring member. This will work for big ring also such as the more number of users in a smart grid. In order to summarize the design of ID-based ring signature with forward security the forward security is the fundamental tool. The key features are:

A. **Data authenticity**:
In the situation of Smart Grid, the statistically usage of energy data would be misleading . While this issue can be solved using well known cryptographic tools for e.g., message authentication code or digital signatures, one may encounter additional difficulties when other issues like anonymity and efficiency are taken into account.

B. Anonymity:
Energy usage data contains large information of consumers, from which one can extract the any number of persons in the home, the types of electric tools used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such type of applications, and any failures to do so may lead to unwillingly to share data of consumers with others.

C. 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.

II. RELATED WORK

An exhaustive literature survey has been conducted to identify related research works conducted in this area. Abstracts of some of the most relevant research works are included below.

A .Identity-based Ring Signature

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

Identity-predicated (ID-predicated) cryptosystems eliminate the desideratum for validity checking of the certificates and the desideratum for registering for a certificate afore getting the public key. These two features are desirable especially for the efficiency and the authentic spontaneity of ring signature, where a utilizer can anonymously sign a message on behalf of a group of spontaneously conscripted users including 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.

B. Forward-Secure Digital Signature Scheme

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.[9]

C. Security and Privacy-Enhancing Multicloud Architectures

Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And Privacy-Enhancing Multicloud Architectures" Member, IEEE, Luigi Lo Iacono

Security challenges are still among the most astronomically immense obstacles when considering the adoption of cloud accommodations. This triggered a plethora of research activities, resulting in a quantity of proposals targeting the sundry cloud security threats. The conception of making utilization of multiple clouds has been distinguishing the following architectural patterns: Replication of applications sanctions to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the utilizer to get evidence on the integrity of the result. Partition of application System into tiers sanctions disuniting the logic from the data. This gives adscititious aegis against data leakage due to imperfections in the application logic. Partition of application logic into fragments sanctions distributing the

application logic to distinct clouds. This has two benefits. First no cloud provider learns the consummate application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality. Partition of application data into fragments sanctions distributing fine-grained fragments of the data to distinct clouds. The fundamental underlying conception is to utilize multiple distinct clouds at the same time to mitigate the jeopardies of maleficent data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust postulation can be lowered to a postulation of non-collaborating cloud accommodation providers. Further, this setting makes it much harder for an external assailant to retrieve or tamper hosted data or applications of a concrete cloud utilizer. These approaches are operating on different cloud accommodation levels, are partly amalgamated with cryptographic methods, and targeting different utilization scenarios.

- Data sharing in multi-cloud environment.
- Data security in multi-cloud.

III. SYSTEM ARCHITECTURE

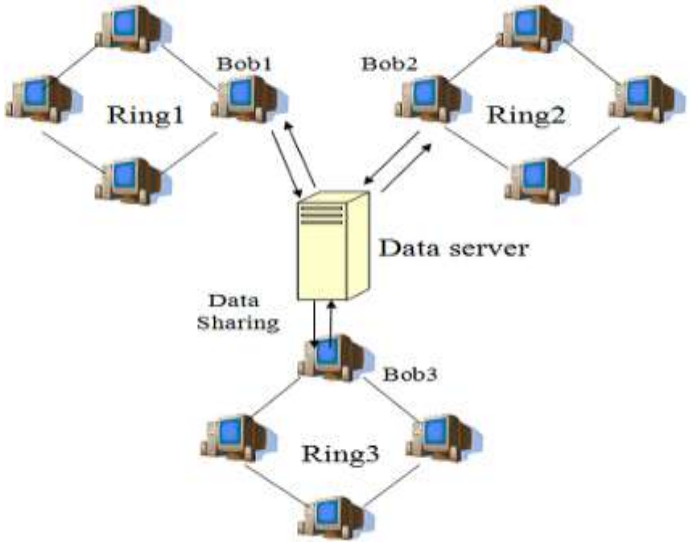

Fig.1.System Architecture

Forwarded secure Identity-based (ID-based) ring signature which eliminates the process of certificate verification which combines ID based system and ring signature. In this project further enhance the security of ID-based ring signature by providing forward security. In this scheme the data or information should be segmented and shared across different location. This property is especially important to any large scaledata sharing system. The key should be used in integer format.

[6] In 2011 C. A. Melchor, et al propose a new efficient "threshold ring signature scheme based on coding theory". Ring signature is one type of group-oriented signature with privacy protection on each user. A user can sign individually on behalf of a group on his own choice and send to the other persons in the group as depicted in Figure . Any verifier can be frustrated that a message has been signed by one of the members in this group also called the Rings but the identity of the user is hided from the originality.

Ring signatures could be used for whistle blowing membership authentication for an ad hoc networks and many other applications which do not want complicated group formation stage but require anonymity signature. There have been many different schemes for ring signature was proposed since the first appearance of ring signature could be published at 1994 [7] and the formal introduction should be given at 2001 in [8].

IV. IMPLEMENTATION

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 $2^l < e < 2^{l+1}$ 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, with identity Idi E (0,1)* requests for a secret key at time period t, where 0 ≤ t < T, the PKG computes the user secret key

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

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 E {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 ≠π , choose random Ai Z*N and compute

$$R_i = A_i^{e^{(T+1-t)}} \bmod N \text{ and } h_i = H_2(\mathcal{L}, m, t, ID_i, R_i)$$

2) Choose random Aπ E Z*N and compute

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

$$h_\pi = H_2(\mathcal{L}, m, t, ID_\pi, R_\pi)$$

3) Compute s= $(sk_\pi, t) h_\pi . \prod_{i=1}^{n} A_i \bmod N$

4) Output the signature for the list of identities L, the message m, and the time period t as

$$\sigma = (R1, \ldots, Rn, h1, \ldots, hn, s).$$

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

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

It outputs valid if all equalities are there otherwise it outputs invalid.

V. RESULT ANALYSIS

A. User registration:

To register a new user, first click on new user. Then registration form will be opened. In this form user has to fill all the registration details that is user name,date of birth, password and email id of user. When user fills all the valid information then click on submit button. If all information is valid then message will displayed “details sent successfully”. This is shown In fig .2.1.

B. Group Creation

Any new user want to create group ,then he has to click on group create. After that new form will opened. Fill all the details of the form. Then message will displayed “group created successfully”. This is shown In fig .2.2.

Fig.2.1 User Registration Fig. Fig.2.2 User Registration

VI. CONCLUSION

Due to the practical needs of data sharing a new notion called forward secure ID-based ring signature is introduced. It combines the ID-based ring signature scheme with forward security.The size of utilizer secret key is just one integer, and the key update process only requires an exponentiation.Cost efficient mechanism is to reduce space and time complexity.

This scheme will be very useful in many other practical applications, especially in ad-hoc network, e-commerce activities and smart grid. These are all requires user privacy and authentication. The current scheme relies on the random oracle model to prove its security. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

REFERENCES

[1] J. K. Liu and D. S. Wong, "Solutions to key exposure problem in ring signature," I. J. Netw. Secur., vol. 6, no. 2, pp. 170–180, 2008.
[2] J. K. Liu, T. H. Yuen, and J. Zhou, "Forward secure ring signature without random oracles," in Proc. 13th Int. Conf. Inform. Commun. Security, 2011, vol. 7043, pp. 1–14.
[3] *H. Xiong, Z. Qin, and F. Li. An anonymous sealed-bid electronic auction based on ring signature. I. J. Network Security, 8(3):235 242, 2009.*
[4] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo. Noninterative forward-secure threshold signature without random oracles. J. Inf. Sci. Eng., 28(3):571586, 2012.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy preserving public auditing for secure cloud storage. IEEE Trans. Computers, 62(2):362375,2013.
[6] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," IEEE Trans. Inform. Theory, vol. 57, no. 7, pp. 4833–4842, Jul. 2011.
[7] R. Cramer, I. Damga rd, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in Proc. 14th Annu. Int. Cryptol. Conf. Adv. Cryptol., 1994, vol. 839, pp. 174–187.
[8] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2001, vol. 2248, pp. 552–565.
[9] 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