ISSN 2348 – 9928
IJAICT Volume 2, Issue 7, November 2015 Doi:01.0401/ijaict.2015.07.04 Published on 05 (12) 2015

FORWARD SECURE IDENTITY BASED RING SIGNATURE SCHEME FOR IMAGES

Ms. S. N. Saranya
PG Scholar,
Sasurie Academy of Engineering,
Coimbatore, Tamilnadu, India

Ms. P. Thilagavathi
Assistant Professor,
Sasurie Academy of Engineering,
Coimbatore, Tamilnadu, India

Ms. M. Tharani
PG Scholar,
Sasurie Academy of Engineering,
Coimbatore, Tamilnadu, 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.

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, key revocation 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.

In a ring signature scheme the key exposure create more severe problem. If the secret key of one of the ring member's is exposed by the attacker means they can produce valid ring signatures of any documents belonging to that group. For doing this type of attack the attacker only needs to include the compromised user in the "group" and silently watch the transaction between the groups. 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 of this forward security scheme is

- It is in ID-based setting so the elimination of the costly certificate verification process makes it scalable for large number of users and especially suitable for big data analytic environment.
- The size of a secret key is just one integer.
- Key update process only requires an exponentiation time.
- The pairing operation could not be used in any stage.

II. EXISTING SYSTEM

[3] In 2010 NIST propose a "Guidelines for Smart Grid Cyber Security". Consumers in Smart Grid share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm. The data of single persons stored within a same block. While at receiving the data of a particular owner should be retrieved from that same block only as depicted in Figure 1

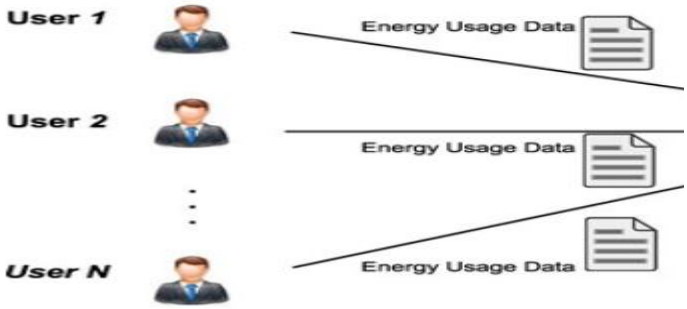

Fig 1:- Grid Structure

Drawback:-

- Ability to access, analyzes, and respond to much more precise and detailed data is computationally slow.
- From all levels of the electric grid the efficient energy usage is critical.
- Due to its openness manner data sharing between users is always deployed in a aggressive environment.
- Vulnerable to a number of security threats.

Also this paper discusses the Major properties Of Data Center and their problem and solution. They are data authenticity, Anonymity, Efficiency, Availability and access control

Data Authenticity:-

Problem:-In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries.

Solution:-While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), one may encounter additional difficulties when other issues are taken into account, such as anonymity and efficiency;

Anonymity:-

Problem: Energy usage data contains vast information of consumer. from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc.

Solution:-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.

Availability:-

There are other security issues in a data sharing system which are equally important, such as availability (service is provided at an acceptable level even under network attacks).

Access Control:-

Only eligible users can have the access to the data

2.1 ID Based Crypto System

[4] In 1984 Shamir et.al propose "Identity-based cryptosystems and signature Schemes". In order to overcome the efficiency, data integrity and privacy issues this identity scheme was introduced. This will be applied on applications requiring data authenticity and anonymity. Identity-based (ID-based) cryptosystem eliminates the need for verifying the validity of public key certificates. The major disadvantage is the management of which is both time and cost consuming.

[5]In 2010 P. P. Tsang, et al proposes "A suite of non-pairing ID-based threshold ring signature schemes with different levels of anonymity". The public key of each user is easily computable from a user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from. This public and private key property avoids the need of certificate validation. This type of validation required necessary in traditional public-key infrastructure and associates an implicit public key i.e. user identity to each user within the system. The ID-based signature

is different from the traditional public key based signature because it requires certificate verification first.

Advantage:-

- The elimination of the certificate validation makes the whole verification process more efficient
- Lead to a significant save in communication and computation when a large number of users are involved (say, energy usage data sharing in smart-grid).

Disadvantage:-

- If the private key of a signer is compromised, all signatures of that signer become worthless:
- Future signatures are invalidated and no previously issued signatures can be trusted.
- Once a key leakage is identified, key revocation mechanisms must be invoked immediately in order to prevent the generation of any signature using the compromised secret key. However, this does not solve the problem of forge ability for past signatures.

2.2 Ring Signature

[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 2. 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 actual 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 signer anonymity. 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].

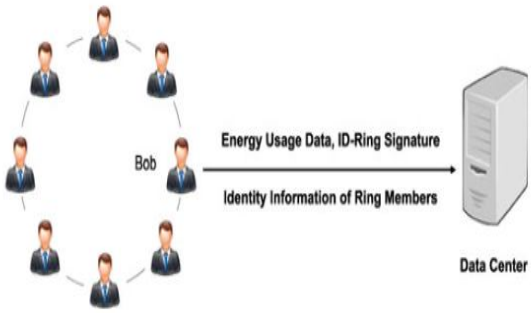

Fig 2:-Multi Identity Based Data Access System

Advantage:-

- Due to its natural framework, ring signature in ID-based setting has a significant advantage over its counterpart in traditional public key setting, especially in the big data analytic environment.
- The first ID-based ring signature scheme was proposed in 2002 [9] which can be proven secure in the random oracle model.
- The selective- ID model could be secure.
- The first ID-based ring signature scheme claimed to be secure in the standard model [10] because it is under the trusted setup assumption.

Drawbacks

- Costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable.
- ID based signatures does not have forward security.
- Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 certificates of the corresponding users, after which one can carry out the actual verification on the message and signature pair which is a costly process, saves a great amount of time and computation.
- This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring.
- However, the proof described in [10] is wrong and is pointed out by [11].

III. PROPOSED SYSTEM

Forwarded secure Identity-based (ID-based) ring signature which eliminates the process of certificate verification which combines the ID Based crypto 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 scale data sharing system. The key should be used in integer format. The same should be used in ring basis at different combinations. Forward Secure ID Based Signature eliminates the costly verification. Private Key generator combines all segments from different location. In this paper, we propose a new notion called forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system. A concrete design is to be designed to create forward secure ID based ring signature. None of the previous

ID-based ring signature schemes in the literature have the property of forward security, and the proposed scheme is the first one which contains this feature. The security of the proposed scheme reviewed in the random oracle model and the standard RSA assumption;

Advantages

- The scalability and flexibility is increased.
- Due to its in directness , data sharing is always deployed in a different location
- To provide security in data sharing
- To provide cost effective forward security
- The security of the proposed scheme is increased by using this random oracle model.

IV. 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. This is the first scheme which combines the forward security with the ring signature in ID-based setting. This scheme provides unconditional security and can be proven forward-secure un forge ability in the random oracle model. This forward scheme is very efficient and does not require any pairing operations. 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.

References

[1] J. K. Liu and D. S. Wong, "Solutions to key exposure problemin 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] NIST IR 7628: Guidelines for Smart Grid Cyber Security, NIST IR7628: Guidelines for Smart Grid Cyber Security, Aug. 2010.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. CRYPTO 84 Adv. Cryptol., 1984, vol. 196, pp. 47–53.

[5] 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.

[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] F. Zhang and K. Kim, "ID-based blind signature and ring signature from pairings," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security, 2002, vol. 2501, pp. 533–547.

[10] J. Han, Q. Xu, and G. Chen, "Efficient ID-based threshold ring signature scheme," in Proc. IEEE/IFIP Int. Conf. Embedded UbiquitousComput., 2008, pp. 437–442.

[11] 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.