International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 6 (June '2016)

FORWARDED SECURE IDENTITY BASED RING SIGNATURE SCHEME WITH SEGMENTED CELLULAR AUTOMATA SCHEMES

S.N.Saranya,
PG Student,
Sasurie Academy of Engineering,
Coimbatore,India.

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

M.Suguna,
Assistant Professor,
Sasurie Academy of Engineering,
Coimbatore,India.

Abstract: In the advanced cloud computing world Data sharing has never been easier task. Data communication with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Cellular automata image is a promising candidate to construct an anonymous and authentic data sharing system. The segmented allows a data owner to anonymously authenticate his data which can be put into the different places of cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Forwarded 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 Forwarded ID-based ring signature by providing with segmented cellular automata scheme. If a secret key of any user has been compromised, all previous generated segments that include with a 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.

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

I. INTRODUCTION

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: 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 Storage at different places with identity information. Forward secure ID-based ring signature, which is an essential tool for building cost-effective authentic and anonymous data sharing system:
ID-based ring signature seems to be an optimal trade-off among efficiency, data authenticity and anonymity, and provides a sound solution on data sharing with a large number of participants. To obtain a higher level protection, one can add more users in the ring. But doing this increases the chance of key exposure as well.

Key exposure is the fundamental limitation of ordinary digital signatures. 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 forgeability for past signatures. The notion of forward secure signature was proposed to preserve the validity of past signatures even if the current secret key is compromised. The concept was first suggested by Anderson and the solutions were designed. The idea is dividing the total time of the validity of a public key into T time periods, and a key compromise of the current time slot does not enable an adversary to produce valid signatures pertaining to past time slots.

Key Exposure in Big Data Sharing System: The issue of key exposure is more severe in a ring signature scheme: if a ring member's secret key is exposed, the adversary can produce valid ring signatures of any documents on behalf of that group. Even worse, the "group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the "group" of his choice. As a result, the exposure of one user's secret key renders all previously obtained ring signatures invalid (if that user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, forward security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource. While there are

various designs of forward-secure digital signatures adding forward security on ring signatures turns out to be difficult. As far as the authors know, there are only two forward secure ring signature schemes [1], [2]. However, they are both in the traditional public key setting where signature verification involves expensive certificate check for every ring member. This is far below satisfactory if the size of the ring is huge, such as the users of a smart grid. To summarize, the design of ID-based ring signature with forward security, which is the fundamental tool for realizing cost-effective authentic and anonymous data sharing, is still an open problem.

Our implementation is practical, in the following ways:

- It is in ID-based setting. The elimination of the costly certificate verification process makes it
- scalable 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.
- We do not require any pairing in any stage.

II.LITERATURE SURVEY

[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

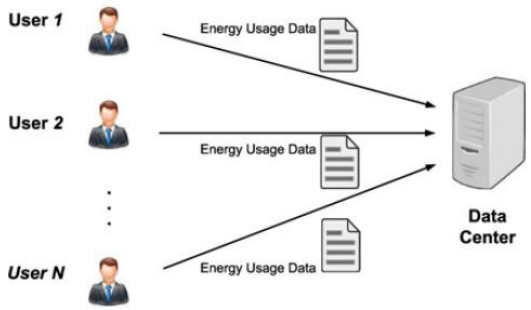

Figure 1:- Grid Structure

Drawback:-

- Ability to access, analyzes, 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.

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

ID Based Crypto System
[4] In 1984 Shamir, propose "Identity-based cryptosystems and signature Schemes".The aforementioned three issues remind us a cryptographic primitive "identity-based ring signature", an efficient solution on applications requiring data authenticity and anonymity. Identity-based (ID-based) cryptosystem, introduced by Shamir [45], eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming.

[5]In 2010 P. P. Tsang, et al propose "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 string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will 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.

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 a group-oriented signature with privacy protection on signature producer. A user can sign anonymously 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 convinced that a message has been signed by one of the members in this group (also called the Rings), but the actual identity of the signer is hidden. Ring signatures could be used for whistle blowing anonymous membership authentication for ad hoc groups and many other applications which do not want complicated group formation stage but require signer anonymity. There have been many different schemes proposed since the first appearance of ring signature in 1994 [7] and the formal introduction in 2001 [8].

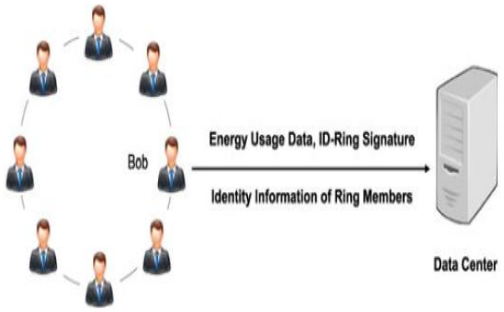

Figure 2:-Multi Identity Based Data Access System

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. Two constructions in the standard model were proposed. Their first construction however was discovered to be flawed [11], while the second construction is only proven secure in a weaker model, namely, selective- ID model. The first ID-based ring signature scheme claimed to be secure in the standard model is under the trusted setup assumption. However, their proof is wrong and is pointed out by [5].

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.

III.EXISTING 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:

For the first time, we provide formal definitions on forward secure ID-based ring signatures;We present a concrete design of forward secure ID based ring signature. No previous ID-based ring signature schemes in the literature have the property of forward security, and we are the first to provide this feature; We prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption;

Advantages of Existing System

- 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.

Disadvantages of Existing System

- Difficult to embed a large amount of message data into a single image.Specifically, if one wants to hide a secret image into a cover image with the same size, the secret image must be highly compressed in advance
- Many applications, such as keeping or transmitting medical pictures, military images, legal documents, etc., that are valuable with no allowance of serious distortions, such data compression operations are usually impractical.

- Requirement of a large image database so that the generated mosaic image can be sufficiently similar to the selected target image.
- Costly certificate verification in the traditional forward security signature setting becomes a bottleneck [8].
- Threshold based signatures does not have forward security[2].
- 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.
- Diffie-Hellman assumption in the standard model situation is even worse for ring signatures, since the attacker can forge a message on behalf of the whole group.
- Moreover, the other members of the group may be completely unaware of such forgery, since they are unaware of being conscripted into the group.
-

IV.PROPOSED SYSTEM

It is aimed to design a new method that can transform a secret image into a secret fragment-visible mosaic image of the same size that has then visual appearance of any freely selected target image without the need of a database. Specifically, after a target image is selected arbitrarily, the given secret image is first divided into rectangular fragments called tile images, which then are fit into similar blocks in the target image, called target blocks, according to a similarity criterion based on color variations. Next, the color characteristic of each tile image is transformed to be that of the corresponding target block in the target image, resulting in a mosaic image which looks like the target image. Then this mosaic image should be embed information like pdf, ppt, and word document and with relevant information for extraction and then the resulting image should be segmented into equal parts along with sub key. The segmented parts and sub key stored into the sub servers and the main key will be given to the Gmail server. If the valid person identified by the Gmail Server then the sub servers provide the segmented parts then by using the sub key the original mosaic image should be reconstructed. From Original mosaic image the secret image and information should be reconstructed based on lossless recovery manner.

Advantages of Proposed System

- This property is especially important to any large scale data sharing system.
- The key should be used in LONG integer format.
- The same should be used in ring basis at different combinations.
- Forward Secure ID Based Signature with ring signature eliminates the costly verification.
- Private Key generator combines all segments from different location.
- For guaranteed communication efficiency and to save network bandwidth, compression techniques can be implemented on digital content to reduce redundancy.
- The quality of the decompressed image should be preserved.
- The combined module increase implementation efficiency. This scheme also be used for the integrity authentication of the images.
- Produce meaningful noise image so attackers hard to detect information.

V.CONCLUSION

Motivated by the practical needs in data sharing, we proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward- secure un forgeable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. Our current scheme relies on the random oracle assumption 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.

VI.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] 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.

[11] A. L. Ferrara, M. Green, S. Hohenberger (2009). Practical short signature batch verification,". Cryptographers' Track RSA Conf. Topics Cryptol., vol. 5473, pp. 309–324

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

