INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Forward secure ID based ring signature for data sharing

Swati Khatal
swati.khatal@gmail.com
Terna Engineering College,
Navi Mumbai, Maharashtra

Tabassum Maktum
tabsmaktum@gmail.com
Ramrao Adik Institute of Technology,
Navi Mumbai, Maharashtra

ABSTRACT

Cloud computing provides services where one can access information from any place, from anywhere, at any time. So basically cloud computing is subscription based service where one can obtain network storage space and computer resources for data storage as well as data sharing. Due to high fame of cloud for data storage and sharing, a large number of participants gets attracted to it. The security is the biggest concern for the adoption of the cloud. The major issues in this regard are efficiency, data integrity, privacy, and authentication. In order to handle these issues concept of a ring, the signature has been introduced for data sharing amongst a large number of users. Ring signatures are used to provide user's anonymity and signer's privacy. But the expensive certificate verification within the ancient Public Key Infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. ID-based ring signature had been introduced which eliminates the process of certificate verification. Further enhancement of security with forwarding security concept has been introduced. According to this idea, if a secret key of any user has been compromised; all previously generated signatures that embrace this user still stay valid. This property is very vital to any giant scale knowledge sharing system because it is not possible to raise all knowledge data owners to re-authenticate their data whether or not a secret key of 1 single user has been compromised. Thus we propose a secure ID-based ring signature with forwarding security.

Keywords— *Authentication, Data sharing, Cloud computing, Forward security*

1. INTRODUCTION

The popularity and enlarged use of cloud make information sharing a lot of convenient information sharing provided additional edges to society.

Example: The smart grid customers can get the energy consumption info yet as they'll share this information with others. This information is uploaded to a 3rd party like Microsoft Hohm. The collected information is compiled within the type of report to a personal will compare the energy consumption with others (e.g., from the identical block). This ability to access, analyze, and reply to far more precise and elaborate information from all levels of the electrical grid is crucial to economical energy usage.

A practical system should satisfy the goals of security. The security goals are:

(a) Data Authenticity: When two systems are communicating with each other, they should authenticate the communication in order to satisfy the security goal. If the systems are not properly authenticated the data can be misused. In the smart grid, the energy usage report would be deceptive if the systems are not authenticated hence adversaries will be able to falsify the data. To solve the authentication problem various cryptographic tools (e.g., a message authentication code or digital signatures) can be used.

(b) Anonymity: Anonymity indicates protection to the user identity. The energy consumption report contains information about a number of consumers in a house, the types of electric appliances used in a specific time period, etc. Thus anonymity is an important factor in security.

(c) Efficiency: As the variety of users are vast in number a value and computation system ought to be designed to scale back the wastage of energy.

We propose "identity-based ring signature" that is an associate economical resolution on applications requiring knowledge credibility and anonymity and security. Its additional strengthen by adding forward security thereto.

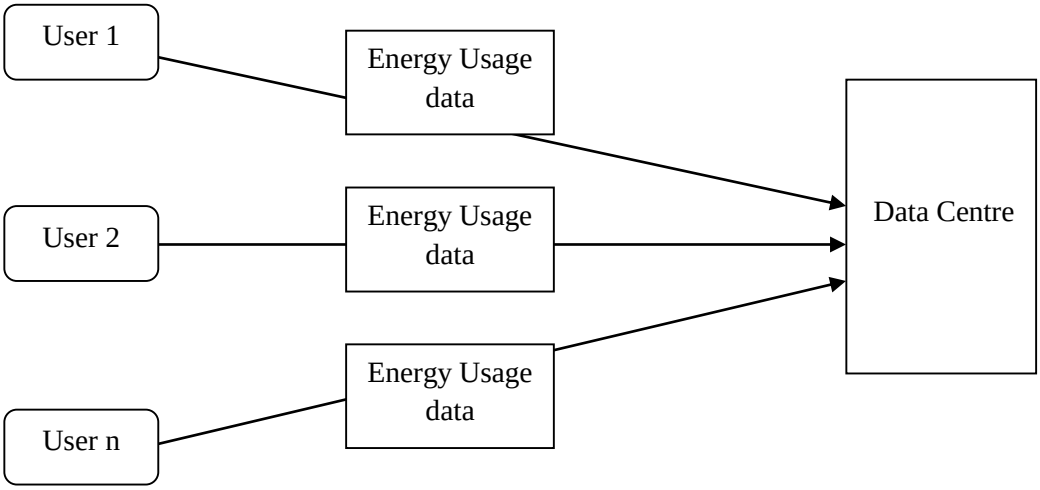

Fig. 1: Energy usage data sharing system

1.1 Applications of forward secure ID-based ring signatures

(a) Smart Grid: Smart Grid is one form of electricity network which is having digital technology. The smart grid is having two-way capabilities for data communication: Not only the grid controller can issue commands to intelligent devices, consumers and devices can also send data to grid controllers. The ability to access, analyze, and answer way more precise and careful information from all levels of the electrical grid is vital to the foremost edges of the smart Grid as an example, Microsoft Hohm provides a platform for consumers to upload energy usage data, based on which a statistical report is created. The purpose is that consumers should compare energy usage with others in order to use electricity more efficiently.For comparison of data, the consumers should reproduce the original data. Hence data integrity is a necessary requirement in these applications. Ring signature is a propitious solution on applications (e.g., Microsoft Hohm) requiring both integrity and privacy. In-ring signature, the service provider will check for a valid signature, without telling who exactly the consumer is. Forward security is surely alluring in this circumstance since a traded off private key inside a timespan won't have any negative effect on measurable reports produced already. At the end of the day, old factual reports would stay legitimate if forward-security is fulfilled.

(b) Whistle Blowing: Suppose in some corporate sector if employee wants to register a complaint regarding higher authority or anyone else they can use forward secure id based ring signature to anonymously send a message to concern person. The admin can verify that message is from an authorized person only though he can't understand who the actual signer is. Forward security enhances the protection of all entities. While not forward security, if the secret key of the member is exposed, each ring signature containing that member within the ring can become invalid. This can greatly have an effect on the accuracy of the knowledge.

2. LITERATURE SURVEY

Sub-linear size ring signature proposed by N. Chandran, J. Groth, and A [1]. This scheme produces a ring or a group of users, which includes the signer. In this ring signature theme that has size O(√N) wherever N is that the range of users within the ring. A further feature of the theme is that its excellent anonymity. Though it provides anonymous authentication it needs costly public key certificate verification.

ID-based Ring Signature from Pairings was proposed by Hung-Yu Chien [3]. This ring signature scheme empowers an underwriter in a specially appointed way to sign a mark in the interest of a gathering of clients including himself with the end goal that a verifier can be persuaded that one of the distinguished clients really created the mark yet he can't recognize the genuine endorser. Though it avoids public key certificate verification key exposure problem occurred.

Non-pairing ID-based threshold ring signature was proposed by P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong [4]. This scheme does not have any bilinear pairing. As it is ID based so, though it avoids public key certificate verification key exposure problem occurred. Here the general public key of every user is often simply known. A private key generator (PKG) and signer then cipher private keys from it. This public-private key property avoids would like of digital certificate validation. ID-Based Ring Signature Scheme with Constant-Size Signature scheme proposed by Chengyu Hu, Pengtao Liu. In this scheme, the size of ring signature depends linearly on the ring size. Also, it was having many security issues.

Threshold ring signature scheme based on coding theory proposed by C. A. Melchor, et al. [5] Ring signature is one type of group-oriented signature with privacy protection on each user. A client can sign exclusively in the interest of a gathering without anyone else decision and send to alternate people in the gathering.

Linkable ring signature scheme proposed by J. K. Liu, W. Susilo, and D. S. Wong [12].In this scheme, the identity of the signer in a ring signature remains anonymous, but two ring signatures can be linked if they are signed by the same signer. Length of the signature depends on the number of members.

Blind Ring Signature Scheme was proposed by Jianhong Zhang, Xue liu [13]. It can provide the anonymity of the signed message, thus, it can realize the private protection of user's transaction information. But the length of the signature depends on the amount of member. Thus, it's an associate open downside to construct a blind ring signature with constant size.

ID-Based Ring Signature Scheme with Constant-Size Signature scheme proposed by Chengyu Hu, Pengtao Liu [14]. In this scheme, the size of ring signature depends linearly on the ring size. Also, it was having many security issues.

Threshold ring signature scheme based on coding theory proposed by C. A. Melchor, et al. [15]. Ring signature is one form of cluster headed signature with privacy protection on every user. A user will sign severally on behalf of a bunch of his own alternative and send to the opposite persons within the group. It protects the system from the attack of ring member modification.

Forward-Secure Digital Signature Scheme Mihir Bellare and Sara K. Miner "A Forward-Secure Digital Signature Scheme" [16] Dept. of Computer Science, & Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA Digital signature theme during which the general public secret is fine-tuned however the key sign language key is updated at customary intervals thus on give forward security property: compromise of the present secret key doesn't alter Associate in Nursing individual to forge signatures regarding the past. This will be helpful to mitigate the injury caused by key exposure whereas not requiring the distribution of keys. The event uses conceptions from the signature schemes and is proved to be forward secure predicated on the hardness of factorization, among the discretionary oracle model. The event is additionally quite economical. Past signature keeps secure whether or not or not expose this secret key.

Security and Privacy-Enhancing multi-cloud Architecture [18] Jen-Matlhians Bohli, Nils Gruschka, Meiko Jenson, "Security and Privacy-Enhancing multi-cloud Architecture" Adaptation of cloud for data sharing and storage faces many security challenges. When data is stored on multiple clouds, its integrity is checked by receiving multiple results from one operation which is performed on different cloud and compare them within own premise. This allows checking the integrity of results. In applications, logic is fragmented to distinct clouds. Its benefit will be no cloud provider will know the entire logic and no cloud provider will learn the entire calculated result of applications and hence maintains application confidentiality.

Table 1. Analysis of different schemes

Authors	Method used	Issues
N. Chandran, J. Groth, and A. Sahai	Sub-linear size ring signature scheme.	Needs public key certificate verification and costly.
Hung-Yu Chien	ID-based Ring Signature from Pairings	Key exposure i.e. If the non-public key of a signer is compromised, all signatures of that signer become worthless: future signatures are nullified and no antecedently issued signatures may be trustworthy
P. P. Tsang, M. H. Au, J. K. Liu, W. Susilo, and D. S. Wong	Non-pairing ID-based threshold ring signature.	Key Exposure
Chengyu Hu, Pengtao Liu	ID-based ring signature scheme with constant-size signature.	Lack of security.
C. A. Melchor, P.L. Cayrel, P. Gaborit, and F. Laguillaumie	Threshold ring signature scheme based on coding theory.	Key Exposure

3. THE PROPOSED SYSTEM

In order to handle the issues in data sharing like data integrity, privacy and efficiency, we propose **"**Forward secure ID-based ring signature**"** scheme, which provides unconditional anonymity with security. Compared to existing schemes, our scheme supports anonymous authentication and also handles the issue of key exposure with the help of forward security.

The proposed method is the implementation of whistleblowing mechanism. The example of employee portal is considered for implementation of the proposed scheme. The employee can register the complaint using a forward secure id based ring signature scheme. According to this scheme, suppose in some corporate sector if employee wants to register a complaint regarding higher authority or anyone else they can use forward secure id based ring signature to anonymously send a message to concern person. The admin can verify that message is from an authorized person only though he can't understand who the actual signer is. Forward security enhances the protection of all entities. Without forward security, if the secret key of member is exposed, every ring signature containing that member in the ring will become invalid. This will greatly affect the accuracy of the information.

The first user has to register to get access to the system. After logging in user have to download the key. The key will be generated by the RSA algorithm. By using the key user will sign the message by using the identity of other users including its own. Because ring signature is a group-oriented signature with privacy protection on the signature producer. A user can sign anonymously on behalf of the cluster on his own different, whereas cluster members are going to be fully unaware of being conscripted at intervals the cluster. Any verifier are going to be convinced that a message has been signed by one altogether the members throughout this cluster (also called the Rings), but the actual identity of the signer is hidden. In Associate in Nursing ID-based cryptosystem, the general public key of every user is well calculable from a string like this user's publically famous identity

(e.g., Associate in a Nursing email address, a residential address, etc.). A personal key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates (which are necessary for ancient public-key infrastructure) Associate in Nursing associates an implicit public key (user identity) to every user within the system. The elimination of the certificate validation makes the full verification method a lot of economical, which can cause a significant save in communication and computation once an oversized variety of users are concerned. The key will be valid for a few time period solely as we tend to are implementing forward security. As per this idea, if a secret key of any user has been compromised; all previously generated signatures that embody this user still stay valid. The idea is dividing the entire time of the validity of a public key into T time periods Associate in Nursing a key compromise of the present time interval doesn't alter an individual to provide valid signatures per diversion slots. This property is very necessary to any giant scale information sharing system because it is not possible to raise all information data owners to re-authenticate their data whether or not a secret key of 1 single user.

3.1 System flowchart

Figure 2 describes the working of the proposed system. The system is divided into different modules like Authentication, Data sharing, Identity-based Ring Signature, and Forward security.

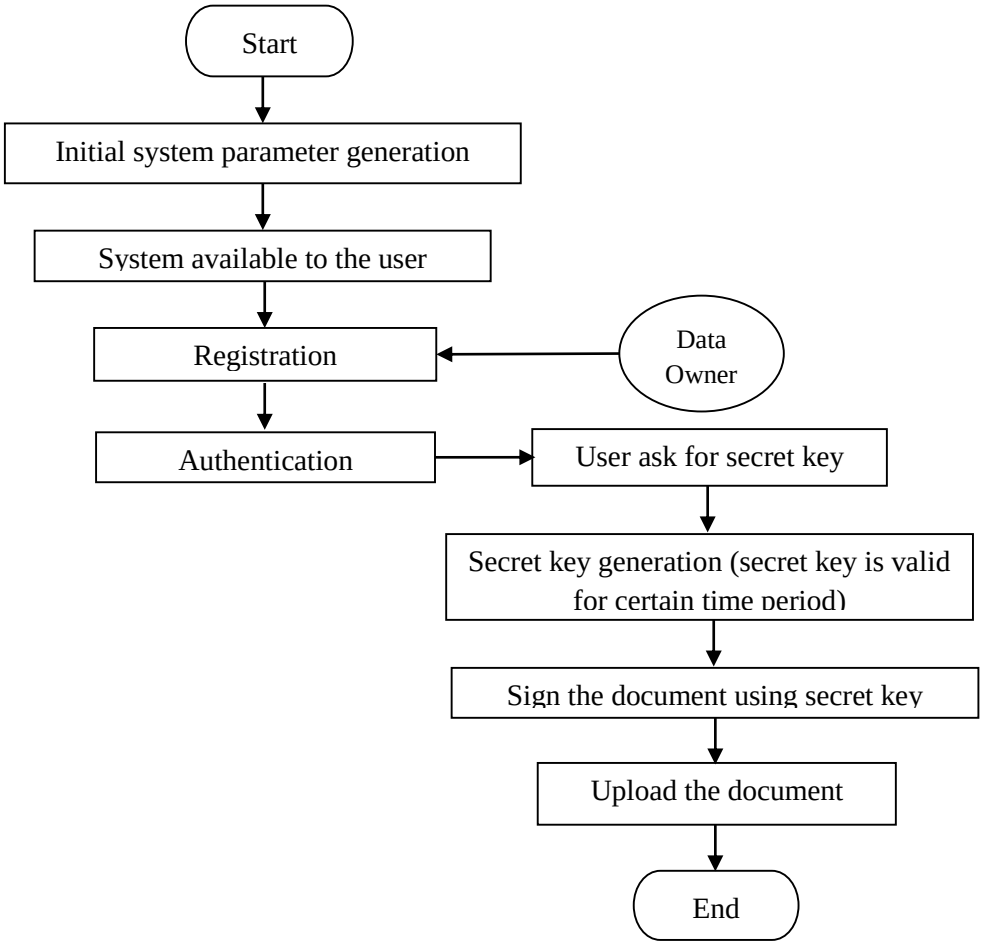

Fig. 2: System flowchart

4. CONCLUSION

Due to the sensible wants of knowledge sharing a new notion referred to as forward secure ID-based ring signature is introduced. It combines the ID-based ring signature theme with forwarding security. Once exploitation this theme user will sign anonymously on behalf of a bunch on his own selection, whereas cluster members will be all unaware of being conscripted within the group. Any verifier will be convinced that a message has been signed by one in all the members during this cluster (also referred to as the Rings), however, the particular identity of the signer is hidden. Forward security provides more security to the current theme wherever, if a secret key of any user has been compromised; all previously generated signatures that embrace this user still stay valid. We'll attempt to scale back the dimensions of user's secret key. Value economical mechanism is to scale back area and time complexness. This theme is going to be very helpful in several alternative sensible applications, particularly in the ad-hoc network, whistleblowing.

5. REFERENCES

[1] N. Chandran, J. Groth, and A. Sahai, "Ring signatures of sublinear size without random oracles," in Proc. 34th Int. Colloq.Automata, Lang. Programming, 2007, vol. 4596, pp. 423–434.

[2] J. K. Liu, V. K. Wei, and D. S. Wong, "A separable threshold ring signature scheme," in Proc. 6th Int. Conf. Inform. Security Cryptol., 2003, vol. 2971, pp. 12–26.

[3] J. Zhang, "An efficient identity-based ring signature scheme and its extension," in Proc. Int. Conf. Comput. Sci. Appl., 2007, vol. 4706, pp. 63–74

[4] 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.

[5] J. K. Liu and D. S. Wong, "Solutions to key exposure problem in ring signature," I. J. Network. Security, vol. 6, no. 2, pp. 170–180, 2008.
[6] 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.
[7] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure multi-owner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.
[8] 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.
[9] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in Proc. 10th Int. Conf. Practice Theory Public Key Cryptography, 2007, vol. 4450, pp. 166–180.
[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forward secure identity-based signature: Security notions and construction," Inform. Sci., vol. 181, no. 3, pp. 648–660, 2011.
[11] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo, "Noninteractive forward-secure threshold signature without random oracles," J. Inform. Sci. Eng., vol. 28, no. 3, pp. 571–586, 2012.
[12] J. Zhang, "An efficient identity-based ring signature scheme and its extension," in Proc. Int. Conf. Comput. Sci. Appl., 2007, vol. 4706, pp. 63–74.
[13] J. K. Liu, W. Susilo, and D. S. Wong, "Ring signature with designated linkability," in Proc. 1st Int. Conf. Security, 2006, vol. 4266, pp. 104–119
[14] 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
[15] 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
[16] 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.
[17] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.
[18] Shamir. "Identity-Based Cryptosystems and Signature Schemes".In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer, 1999.
[19] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security and Privacy-Enhancing Multi-cloud Architectures" Member, IEEE, Luigi Lo Iacono.

