Volume 2, Issue 12, December-2015, pp. 1126-1131 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

[1]C.Praveen Kumar, [2]P Suman Prakash, [3]Dr.S.Prem Kumar

[1]*Pursuing M.Tech, CSE Branch, Dept of CSE*

[2]*Assistant Professor, Department of Computer Science and Engineering*

[3]*Professor & HOD, Department of computer science and engineering, G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.*

Abstract—Data distribution is not at all easier with the progress of cloud computing, and an exact examination on the shared data offers a collection of profits both to the the public and individuals. Data distribution with a huge number of applicants must get into account numerous issues, counting effectiveness, data integrity and confidentiality of data owner. Ring signature is a capable applicant to build an unsigned and genuine data sharing system. It lets a data owner to secretly authenticate his data which can be set into the cloud for storage or scrutiny purpose. so far the expensive certificate authentication in the conventional public key infrastructure (PKI) surroundings becomes a restricted access for this solution to be scalable. Identity-based (ID-based) ring signature, which eradicates the method of certificate verification, can be utilized instead. In this paper, we additionally improve the safety of ID-based ring signature by giving advance security: If a secret key of any user has been compromise, all earlier produced signatures that contain this user still remains legal. This property is particularly significant to any huge scale data distribution system, since it is unfeasible to request all data owners to re-authenticate their data still if a secret key of one single user has been compromised. We offer an actual and well-organized instantiation of our scheme, demonstrate its safety and supply an accomplishment to illustrate its realism.

Keywords—cloud computing, forward security, smart grid, data distribution, Authentication

1. INTRODUCTION

The fame and extensive use of "CLOUD" have carried great handiness for data sharing and gathering [8]. Not only can persons obtain helpful data more easily, sharing data with others can give a quantity of profit to our public as well [14]. As a envoy example, clients in Smart Grid can acquire their energy practice data in a fine-grained manner and are habitude to distribute their personal energy usage data with others, e.g., by uploading the information to a third party plat-form which is shown in (Fig. 1). From the collected data a statistical description is produced, and one can evaluate their energy usage with others i.e. from the same block. This skill to access, examine, and reply to much more accurate and full data from all stages of the electric grid is dangerous to well-organized energy usage. Appropriate to its directness, data sharing is at all times organized in an aggressive atmosphere and susceptible to a quantity of security fears. Considering energy utilizing data sharing in Smart Grid as a model, there are numerous security objectives to a practical system must meet, as well as:

i) **Competence:** The amount of clients in a data sharing system could be vast and a realistic system must decrease the calculation and communication cost as much as possible. Or else it would guide to a misuse of energy, which oppose the objective of smart grid.

ii) **Data genuineness**: If we consider the condition of smart grid, the statistic energy usage data might be ambiguous if it is fake by opponents. Whereas this subject on your its can be resolved using well recognized cryptographic tools for eg. Digital signatures, one may come across extra difficulties at the time of other problems are considered into account, such as secrecy and effectiveness.

Secrecy: Energy usage information includes vast data of customers, as of which one can take out the quantity of people in the residence, the types of electric utilities used in a exact time period, etc. Therefore, it is dangerous to safe guard the secrecy of customers in such requests, and any malfunctions to do so may lead to the reluctance from the customers to divide data with others.

This document is dedicated to examining basic security tools for understanding the three properties we expressed. It is to be noted that there are further security issues in a data sharing system which are uniformly significant, such as accessibility i.e. service is offered at a tolerable level even under network attacks and access control i.e. only appropriate users can include the access to the data.

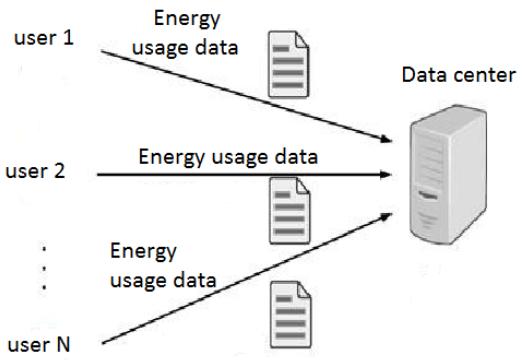

Fig. 1. Energy usage data sharing in smart grid.

1.1 Identity-Based Ring Signature

The abovementioned three topics tell us a cryptographic fundamental "identity-based ring signature" and well-organized solution on request involving data accuracy and secrecy.

1.1.1 ID-Based Cryptosystem

Identity-based (ID-based) cryptosystem, initiated by Shamir, eradicated the need for confirming the authority of public key certificates, the administration of which is both time and cost consuming. In this cryptosystem, the public key of each user is easily assessable from a string corresponding to the user publicly

Known identity (e.g., an email address, a housing address, etc.). A private key generator (PKG) then calculates private keys from its master secret for users. This functionality keeps away from the need of certificates (which are essential in traditional public-key structure) and connects an implicit public key (user identity) to each user within the system. The categorization to verify an ID-based signature, dissimilar from the traditional public key based signature, individual does not need to verify the certificate first. The removal of the certificate support makes the whole confirmation process more capable, which will lead to a significant save in communication and computation while a large number of users are implicated.

Ring signature is nothing but group-oriented signature with privacy security on signature creator. A client can sign secretly on behalf of a group on his own option, as group members can be totally ignorant of being recruited in the group. Any verifier can be influenced that a message has been signed by one of the members in this group (also called the Rings), but the real identity of the signer is hidden. These Ring signatures might be worn for whistle blowing, secret membership verification for adhoc groups [11] and many other requests which do not want complex group structure stage but require signer anonymity. Owing to its natural structure, ring signature in ID-based background has a major benefit over its complement in traditional public key setting.

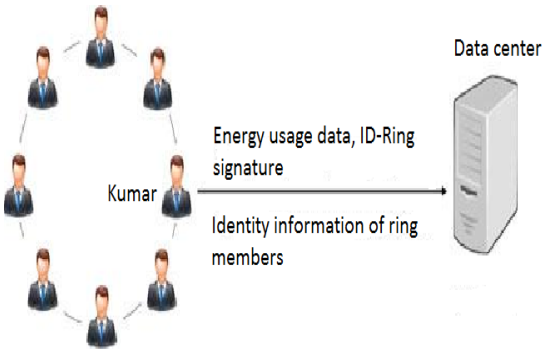

Fig. 2. A solution based on ID-based ring signature.

1.1.2 A Positive Advantage in Big Data

Owing to its usual framework, ring signature in ID-based set-ting has a major advantage over its matching part in traditional public key setting, particularly in the big data analytic environment.

Let us consider an example. Assume there are

20,000 clients in the ring; the verifier of a traditional public key based ring signature should first authenticate 20,000 certificates of the matching clients, following which one can take out the real confirmation on the message and signature pair. On the other side, to confirm an ID-based ring signature, simply the identities of ring users, jointly with the pair of message and signature are required. Since one can observe, the removal of certificate validation, which is a expensive process, consumes a huge amount of time and calculation. This consuming will be more dangerous if a higher level of secrecy is desirable by raising the number of users in the ring. Therefore, as depicted in Fig. 2, ID-based ring signature is more suggestible in the setting with a large number of clients such as energy data sharing in smart grid:

i) Step 1: The energy data vendor (say, kumar) initially setups a ring by selecting a group of users. This stage just requires the public identity details of ring members, such as house addresses, and kumar does not need the consent from any ring members.

ii) Step 2: kumar uploads his personal data of electronic usage, together with a ring signature and the identity information of all ring members.

iii) Step 3: By confirming the ring signature, one can be confident that the data is to be sure given out by a suitable resident (from the ring members) as cannot figure out who the resident is. Therefore the secrecy of the data supplier is making sure mutually with data genuineness. In the meantime, the confirmation is well-organized which does not engage any certificate confirmation. The first ID-based ring signature scheme was projected in 2002 which can be confirmed secure in the random oracle model. Two structures in the regular model were projected .Their first structure however was exposed to be defective [24], while the second structure is only demonstrated safe in a weaker model, explicitly, selective-ID model.

1.2 The inspiration:

1.2.1 Key publicity:

ID-based ring signature appears to be a finest trade-off between effectiveness, data accuracy and secrecy, and offers a sound explanation on data sharing with a large number of applicants. To get a higher level security, one can add additional users in the ring. Other than doing this raises the possibility of key publicity as well.

Key publicity is the basic drawback of common digital signatures. If the private key of a signer is compromised, all signatures of that signer turn out to be valueless: future signatures are cancelled and no earlier issue signatures can be trusted. Previously a key outflow is recognized, key revocation methods must be raised directly in order to stop the generation of any signature using the compromised secret key. On the other hand, this does not solve the trouble of forge ability for earlier signatures.

The idea of further secure signature was planned to protect the validity of past signatures still if the existing secret key is compromised. The idea was first recommended by Anderson [2], and the explanations were intended by Bellare and Miner [7]. The thought of that explains as separating 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 permit an opponent to create valid signatures pertaining to early time slots.

1.2.2 Key publicity in Big Data Sharing System

The topic of key publicity is harsher in a ring signature system: if a ring member's secret key is exposed, the opponent can turn out valid ring signatures of any ID on behalf of that group. Even worse, the "group" can be defined by the opponent at will due to the naturalness property of ring signature: The opponent only wants to include the com-promised user in the "group" of his option. As a consequence, the exposure of one user's secret key cause to be all earlier obtained ring signatures invalid (if that user is one of the ring members), as one cannot discriminate whether a ring signature is produced prior to the key publicity or by which user. So, advance security is a necessary constraint that a big data sharing system must meet. Or else, it will direct to an enormous waste of time and supply.

Though there are a variety of models of forward-secure digital signatures counting advanced security on ring signatures turns out to be difficult.

1.3 Involvement

In this paper, we propose a new idea called advanced secure ID-based ring signature, which is

a necessary tool for building cost-effective reliable and unspecified data sharing system:

i) Intended for the first time, we offer proper definitions on forward secure ID-based ring signatures.

ii) We present a concrete plan of forward secure ID-based ring signature. No earlier ID-based ring signature system in writing have the property of Forward security and we are the first to provide this feature

Our achievement is sensible, in the following behaviors:

1) It is in ID-based setting. The eradication of the expensive certificate verification procedure creates it scalable and particularly appropriate for big data logical surroundings.

2) The size of a secret key is only one integer.

3) Key modifies procedure only need an exponentiation.

4) We do not need any coupling in any phase.

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

ID-based forward secure ring signature scheme are designed to following ways. The identities and user secret keys are valid into T periods and makes the time intervals public and also set the message space M= { 0,1 }*.

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 $2^{\ell} < e < 2^{\ell+1}$ 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, where i Z, with identity IDi {0,1}* requests for a secret key at time period (denoted by an integer), where 0 ≤t < T, the PKG computes the user secret key using its knowledge of the factorization of N.

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

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 {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#,choose random

$R_i = A_i\, e^{(x+1-t)} \bmod N$ and $h_i = H_2(L, m, t.ID, R_i)$

2) choose random A Z*N and compute

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

3) Compute s= (sk t)h $\Pi^{n}_{i=1} A_i \bmod N$

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

= (R_1,…..,R_n,h_1,….,h_n,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

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

Output valid if all equalities hold otherwise output invalid

3. CONCLUSION

Inspired by the realistic requirements in data sharing, we proposed a new idea called forward secure ID-based ring signature. It permits an ID-based ring signature scheme to have advanced security. It is the first in the literature to have this characteristic for ring signature in ID-based

setting. Our system affords unconditional secrecy and can be verified forward security. Our idea is very well-organized and does not require any pairing operations. The size of client secret key is just one integer, while the key update process just needs an exponentiation. We consider our system will be very useful in many other realistic applications, particularly to those needed user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid.Our present scheme relies to show the 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] 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.

[2] 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.)

[3] 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.

[4] 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

[5] A. K. Awasthi and S. Lal, "Id-based ring signature and proxy ring signature schemes from bilinear pairings," CoRR, vol. abs/cs/ 0504097, 2005.

[6] 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. Cryptographic Techn., 2003, vol. 2656, pp 614–629

[7] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666,

[8] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.

[9] A. Boldyreva, "Efficient threshold signature, multisignature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice PublicKey Cryptography: Public Key Cryptography, 2003, vol. 567, pp. 31–46.

[10] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in

Proc. Annu. Int. Cryptol. Conf. Adv. Cryptol., 2004, vol. 3152, pp. 41–55.

[11] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryp-tol. Conf. Adv. Cryptol., 2002, vol. 2442, pp. 465–480.

[12] J. Camenisch, "Efficient and generalized group signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 1997, vol. 1233, pp. 465–479.

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

[14] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," IEEE Trans.Serv.Comput.,vol.5,no.4,pp.551–563,FourthQuarter2012.

[15] D. Chaum and E. van Heyst, "Group signatures," in Proc. Work-shop Theory Appl.

Cryptographic Techn., 1991, vol. 547, pp. 257–265.

[16] L. Chen, C. Kudla, and K. G. Paterson, "Concurrent signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027,
pp. 287–305.

[17] H.-Y. Chien, "Highly efficient ID-based ring signature from pairings," in Proc. IEEE Asia-Pacific Serv. Comput. Conf., 2008,

pp. 829–834.

[18] S. S. Chow, R. W. Lui, L. C. Hui, and S. Yiu, "Identity based ring signature: Why, how and what next," in Proc. 2nd Eur. Public Key Infrastructure Workshop, 2005, vol. 3545, pp. 144–161.

[19] S. S. M. Chow, V.K.-W. Wei, J. K. Liu, and T. H. Yuen, "Ring sig-natures without random oracles," in Proc. ACM Symp. Inform., Comput., Commun. Security, 2006, pp. 297–302.

[20] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, vol. 3531, pp. 499–512.

[21] R. Cramer, I. Damgard, 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.

[22] R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption," in Proc. ACM Conf. Comput. Commun. Security, 1999, pp. 46–51.

[23] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in Ad Hoc groups," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, vol. 3027, pp. 609–626.

[24] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen. (2009). Practical short signature batch verification," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., vol. 5473, pp. 309– 324 [Online]. Available: http://eprint.iacr.org/2008/015

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

