INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 1 (2017) PAGES 1640 - 1647
RECEIVED : 15.02.2017 PUBLISHED : 26.02.2017

RELIABLE CLOUD DATA SHARING WITH IMPROVED SECURITY AND EFFECTIVE COST USING RING SIGNATURE

Shalini.S[1], Praveena.G[2]

[1] PG Student, Dept. of Computer science and Engineering, Priyadarshini Engineering College, Vaniyambadi,Tamilnadu, India,

[2] Associate Professor, Dept. of Computer science and Engineering, Priyadarshini Engineering College, Vaniyambadi, Tamilnadu, India.

Abstract

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. 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 sharing of Information in a cloud environment is inevitable in onward of cloud computing environment. Security in accessing cloud information has to consider many issues such as authentication, cost, time in uploading and many other criteria. Authentication of data is must for utilizing the others data and uploading our own data has become tedious. Getting Certificate and for every access is long process and cost increases. The costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. 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 ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this 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. Forward Security re-authentication overhead is avoided in Ring Signature by using RSA Algorithm we further provide increased level of security in reduced time, efficient and simple manner.

Keywords: Authentication, data sharing, cloud computing, Increased Security.

1. 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 as 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.

2. RING SIGNATURE

In cryptography, a ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup. Ring signatures were invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced at ASIACRYPT in The name "ring signature" comes from the ring-like structure of the signature algorithm.

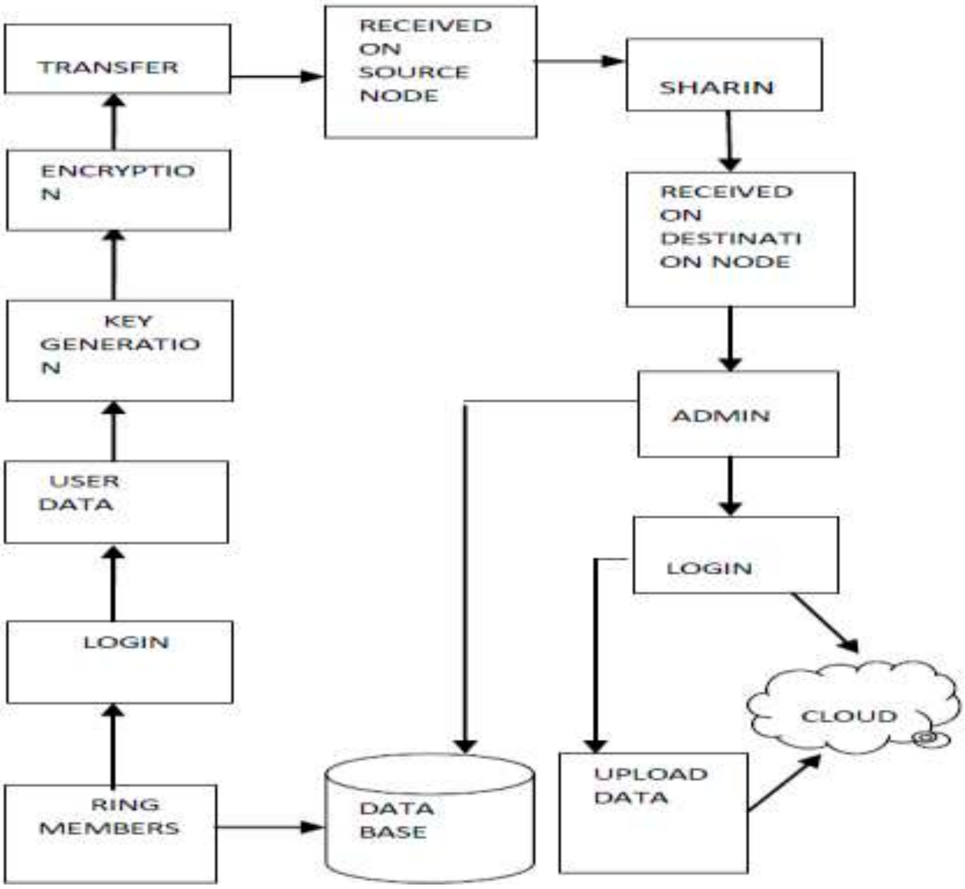


Fig.1. Forwarded Ring

Identity-based Ring Signature

Three issues remind us cryptographic Primitive “Identity-based ring signature”,an efficient solution on applications requiring data authenticity and anonymity.

ID-based Cryptosystem

Identity-based (ID-based) cryptosystem, introduced by Shamir, eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID-based cryptosystem, 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) Associates an implicit public key to each user with in 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 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, while group members can be totally unaware of being conscripted in the group. 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.

An Affirmative Benefits in Big Data

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. Suppose there are 10000 users in the ring, the verifier of a traditional public key based Ring signature must first validate 10000 certificates of the Corresponding users, after which one can carry out the actual verification on the message and signature pair. In Contrast, to verify an ID-based ring signature, only the Identities of ring users, together with the pair of message And signature are needed. As one can see, the elimination of certificate validation, 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. Thus, as depicted based ring signature is more preferable in the setting with a large number of Users such as energy data sharing in smart grid:

Step 1: The energy data owner (say, Bob) first setups a ring by choosing a group of users. This phase only needs the public identity information of ring members, such as residential addresses, and Bob does not need the collaboration from any ring members.

Step 2: Bob uploads his personal data of electronic Usage, together with a ring signature and the identity information of all ring members.

Step 3: By verifying the ring signature, one can be Ring signature is a group oriented signature with assured that the data is indeed given out by a valid resident (from the ring members) while cannot figure out who the Resident is. Hence the anonymity of the data provider is ensured together with data authenticity meanwhile, the verification is efficient which does not involve any certificate verification.

The ID-based ring signature scheme was proposed in 2002. This can be proven secure in the random oracle model. Two constructions in the standard model were proposed in. Their first construction however was discovered to be flaw 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 due to Hanetal. under the trusted set up assumption.

The Motivation

Key Exposure 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 forgetability 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 by Bellare and Miner. 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 timeslot 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 is only two forward secure ring signature schemes .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.

Contribution

In this paper, we propose increased security in ID-based Ring Signature, which is an essential tool for building time reducing cost-effective authentic and anonymous data sharing system: Provided formal definitions on forward secure ID-based ring signatures; In a present concrete design of forward secure ID based ring signature. In the literature have the property of forward security, and prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption; and implementation, in the following ways:

- 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. do not require any pairing in any stage.
- Improved security in uploading in reduced time.

3. DEFINITION

Mathematical Assumption

Definition 1 (RSA Problem): Let $N = pq$, where p and q are two k-bit prime numbers such that $p = 2p + 1$ and $q = 2q + 1$ for some primes p, q. Let e be a prime greater than 2 for some fixed parameter, such that $\gcd(e; \phi(N)) = 1$. Let y be a random element in Z^*N.

We say that an algorithm S solves the RSA problem if it receives an input the tuple $(N; e; y)$ and outputs an element z such that $z = y \bmod N$.

Ring Signature Scheme with Increased Security and reduced Time

The description and analysis of our proposed increased forward secure ring signature scheme as follows.

The Design

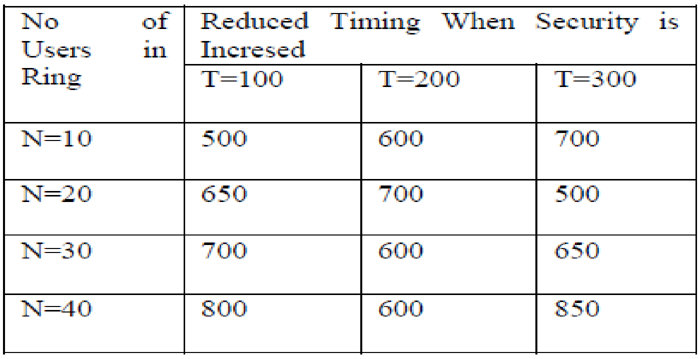
The identities and user secret keys are valid into T periods and make the time intervals public also set the message space M= {0 ,1}*. Setup the PKG generates two random k-bit prime numbers p and q such that p = 2p +1 and q = 2q +1 where p; q are some primes. It computes N = pq. Extract. For user i, where i Є Z, with identity IDi Є {0; 1}* requests for a secret key at time period t (denoted by an integer), where 0 < t < T, the PKG computes the user secret key ski;t = [H1(IDi)] e(T+1t) mod N Update. On input a secret key ski;t for a time period t,if t < T the user updates the secret key.

Sign. To sign a message m Є {0; 1}* in time period t, where 0 < t < T, on a ring of identities L = {ID1,…., IDn}, a user with identity IDπ Є L and secret key skπ,t: Verify. To verify a signature for a message m, a list of identities L and the time period t.

Implementation and Experimental Results

The performance of this scheme with respect to three entities: the private key generator (PKG) for increased security, the data sharer (user), and the service provider (data center). In the experiments, the programs for three entities are implemented using the public cryptographic library MIRACL programmed in C++. All experiments were repeated 100 times to obtain average results shown in this paper, and all experiments were conducted for the cases of |N| =1024 bits and |N| =2048 bits respectively.

The average time for the PKG to setup the system, where the test bed for the PKG is a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon Dual-core dual-processor with 12GB RAM and running Windows 7 Professional 64-bit operating system. It took 151 ms and 2198 ms for the PKG to setup the whole system for |N| = 1024 bits and |N| =2048 bits respectively.



No of Users in Ring	Reduced Timing When Security is Incresed		
	T=100	T=200	T=300
N=10	500	600	700
N=20	650	700	500
N=30	700	600	650
N=40	800	600	850

Unit: ms
Parameters: |N|=1024,|K|=512 (a)

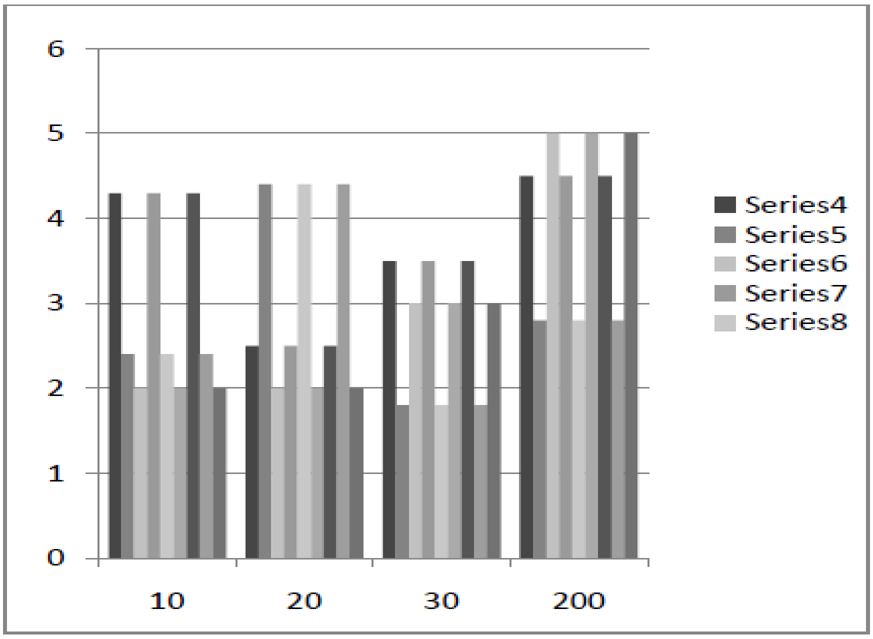


Fig. 2.The number of users in the ring

Fig: The average time for the data owner to sign Energy usage data, |N|=1024

E-CONTRACT SIGNING: A 1-out-of-2 ring signature (containing two users in the ring) can be used to construct concurrent signature. A concurrent signature allows two entities to produce two signatures in such a way that, from the point of view of any third party, both signatures are ambiguous with respect to the identity of the signing party until an extra piece of information (the keystone) is released by one of the parties. Upon release of the keystone, both signatures become binding to their true signers concurrently.

CONCLUSION AND FUTURE WORK

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 proposed a new notion called forward secure ID-based ring signature. It allows an ID-based ring signature scheme to have forward security And Image hiding key transfer. It is the first in the literature to have this feature for ring signature in ID-based setting and hiding key transfer based setting. Our scheme provides unconditional anonymity and can be proven forward secure unforgivable 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. 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 For the future enchantment we can implement everyone can get the admin authentication with some more security enchantment using.

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), pp: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), pp:571-586, 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), pp:362-375,2013.

[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.

[10] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

[11] R. Morris, K. Thompson, "Password security: A case history," Comm. ACM, Vol.22, No. 11, Nov. 1979, pp. 594-597.

[12] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011.