RESEARCH ARTICLE OPEN ACCESS

Increasing Security Level in Data Sharing Using Ring Signature in Cloud Environment

Mrs S.Arogya Swarna, Ms.Shirin Ayisha Maryam.M
Assosciate Professor and HoD/PG CSE S.Veerasamy Chettiar College of Engineering Puliangudi
Assistant Professor/CSE S.Veerasamy Chettiar College of Engineering Puliangudi

Abstract
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. Ring signature gives an assurance to the user to build an unidentified and accurate information sharing system. It allows a data individualistic to innominate authenticate his data which can be put into the cloud for storage or analysis purpose. In Identity-Based (ID Based) Ring Signature Members of this cluster can easily share data avoiding the pricey certificate verification as done in the usual procedure. 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.

I. INTRODUCTION

In cloud computing, there are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers and security issues faced by their The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

The popularity and widespread use of "CLOUD" has brought great convenience for data sharing and collection. Not only can individuals acquire useful data more easily, sharing data with others can provide a number of benefits to our society as well As a representative example, consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a third party platform such as Microsoft Hohm . From the collected data a statistical report is created, and one can compare their energy consumption with others (e.g., from the same block). This ability to access, analyze, 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. Taking energy usage data sharing of security threats. Sharing in Smart Grid as an example, there are several security goals a practical system must meet, including:

Reliability of data:

The situation of Smart Grid, the statistic energy usage data being misleading if it is forged by adversaries. While this issues alone can be solved using well established cryptographic tools, one may encounter additional difficulties when other issues are taken into account, such as anonymity and ability.

Unsingularity:

Energy usage data contains large data of consumers, from which summary the number of persons in the home, variety of electric utilities used in a specific time period It is critical to protect the anonymity of consumers applications, and any failures to do so may lead to the reluctance from the consumers to share data with others.

Effectiveness:

The many users in a information sharing System could be large and a practical system must reduce. The computation and communication cost as much as possible. Otherwise it would lead to a waste of energy, which contradicts the goal of Smart Grid. To investigating fundamental security tools for realizing the three properties we described. Note that there are other security issues in a information sharing system which are equally important, such as availability and access control.

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.

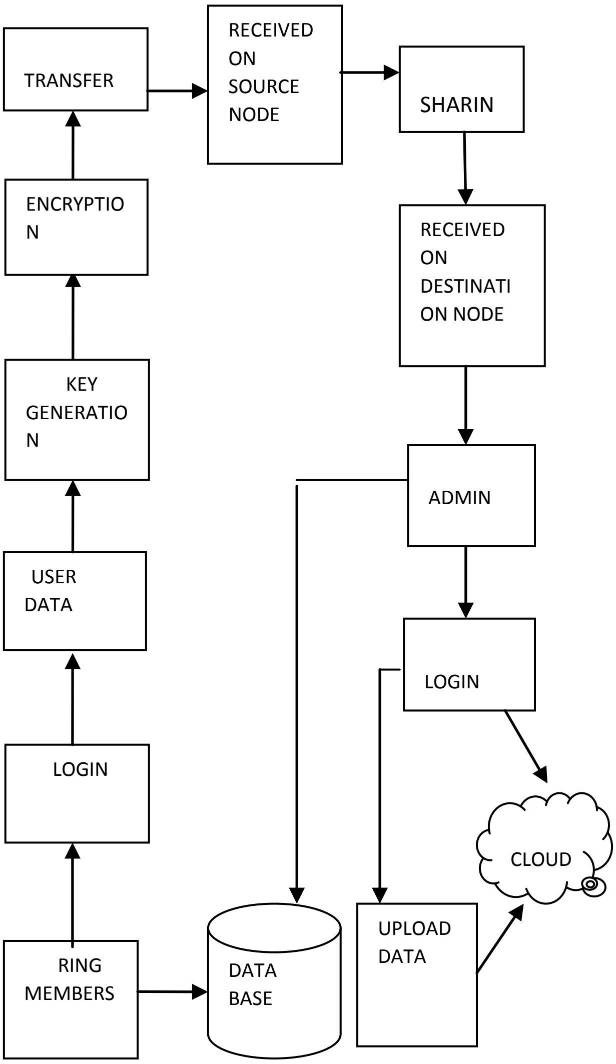


Fig: 1 System Architecture

1.1 Identity-based Ring Signature

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

1.1.1ID-basedCryptosystem

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.

1.1.2An 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 , ID-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 Mean while, 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.

1.2TheMotivation

1.2.1Key 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

1.2.2 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.

1.3 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.

II. DEFINITION

2.1 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; ϕ(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 mod N.

3 Ring Signature Scheme with Increased Security and reduced Time

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

3.1 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
$ski;t = [H1(IDi)]\overline{e(T+1\square t)} \bmod N$

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.

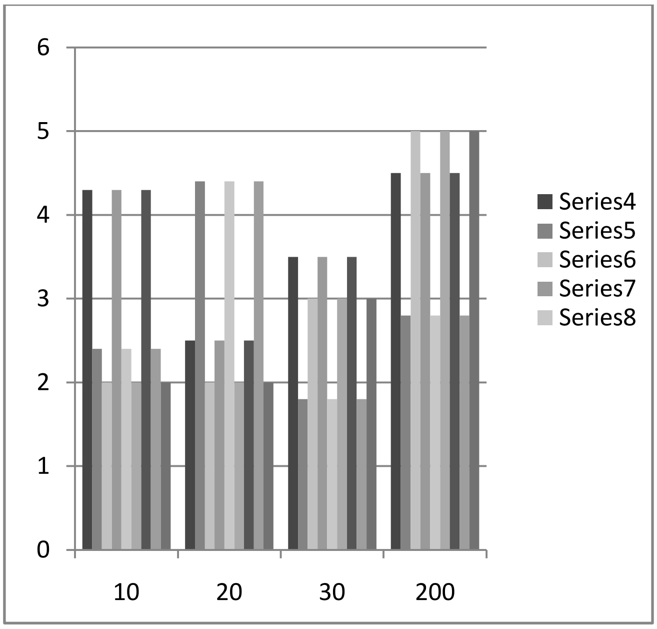
Implementation and Experimental Results

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)



The number of users in the ring
(b)
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

E-AUCTION: Similar to e-contract signing, ring signature schemes can be used to construct e-auction protocols by using ring signature, a winner-identifiable anonymous auction protocol can be build efficiently. That is to say, the auctioneer can authenticate the real identity of the winner at the end of the protocol without additional interactions with the winning bidder even though all the bidders bid anonymously

III. CONCLUSION AND FUTURE ENHANCEMENT

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 unforgeable 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. To improve security for authentication on ring members using MAC algorithm. SHA-1 and MD5 algorithm is used for data encryption. In this algorithm is used for large size of data should be encrypted. sharing data on one ring members to another ring members. Then enhance security on data sharing and upload the data on cloud. 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.] Xinyi Huang, Joseph K. Liu+ Cost-Effective Authentic and Anonymous Data Sharing with Forward Security,2014.

[2.] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong. Id-based ring signature scheme secure in the standard model. In IWSEC, volume 4266 of Lecture Notes in Computer Science, pages 1–16. Springer, 2006.

[3.] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau. Security and privacy-enhancing multicloud architectures. IEEE Trans. Dependable Sec. Comput., 10(4):212–224, 2013.

[4.] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana. Social cloud computing: A vision for socially motivated resource sharing. IEEE T. Services Computing, 5(4):551–563, 2012.

[5.] J. Han, Q. Xu, and G. Chen. Efficient id-based threshold ring signature scheme. In EUC (2), pages 437–442. IEEE Computer Society, 2008.

[6.] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst., 24(1):131–143, 2013.

[7.] J. K. Liu, T. H. Yuen, and J. Zhou. Forward secure ring signature without random oracles. In ICICS, volume 7043 of Lecture Notes in Computer Science, pages1- 14. Springer, 2011.

[8.] 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., 24(6):1182–1191, 2013

[9.] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie. A new efficient threshold ring signature scheme based on coding theory. IEEE Transactions on Information Theory, 57(7):4833–4842, 2011

[10.] H. Shacham and B. Waters. Efficient ring signatures without random oracles. In Public Key Cryptography, volume 4450 of Lecture Notes in Computer Science, pages 166–180. Springer, 2007.

[11.] S. Sundareswaran, A. C. Squicciarini, and D. Lin. Ensuring distributed accountability for data sharing in the cloud. IEEE Trans. Dependable Sec. Comput., 9(4):556–568, 2012.

[12.] 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 ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166–183. Springer, 2010.

[13.] Y. Wu, Z. Wei, and R. H. Deng. Attribute-based access to scalable media in cloud-assisted content sharing networks. IEEE Transactions on Multimedia, 15(4):778–788, 2013.

[14.] G. Yan, D. Wen, S. Olariu, and M. Weigle. Security challenges in vehicular cloud computing. IEEE Trans. Intelligent Transportation Systems, 14(1):284–294, 2013.

[15.] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forwardsecure identity-based signature: Security notions and construction. Inf. Sci., 181(3):648–660, 2011.

[16.] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo. Noninteractive forward-secure threshold signature without random oracles. J. Inf. Sci. Eng., 28(3):571–586, 2012.

[17.] Amit K Awasthi and Sunder Lal. ID-based Ring Signature and Proxy Ring Signature Schemes from Bilinear Pairings. eprint.iacr.org/2004/184.pdf

[18.] 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):362–375, 2013