ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Secure Data Sharing With Linkable Ring Signatures

Anisha S, Neethu Maria John

PG Scholar, Dept. of CSE, Mangalam College of Engineering, Mahatma Gandhi university, Ettumanoor, Kottayam, Kerala, India

Assistant Professor, Dept. of CSE , Mangalam College of Engineering, Mahatma Gandhi university, Ettumanoor, Kottayam, Kerala, India

ABSTRACT: Data distribution is not easier with the use of cloud computing, and an exact analysis on the shared data provides more profit to both the world and individuals. Data distribution with a large number of participants must take into account many issues, that is competence, data reliability and privacy of data owner. Ring signature is a capable candidate to build an unidentified and authentic data distribution system. It allows a data owner to secretly authenticate the data which can be stored into the cloud or study purpose. Yet the most cost consuming certificate verification for public key (PKI) setting becomes a blockage for this solution to be scalable. Identity-based (ID-based) ring signature, which reduces the process of certificate authentication, can be used instead .Here, further improved the security of ID-based ring signature by providing forward security. If a secret key of any user has been leaked, all previous generated digital signatures that include this user still remain valid. This property is basically important to any big data sharing system. Additional methods are implemented to ensure that two users are controllably linkable.

KEYWORDS: Authentication, data sharing, cloud computing, forward security, linkability

I. INTRODUCTION

In cloud computing, there are a number of security issues are associated. The responsibility of the contributor must make sure that their infrastructure is secure and that their clients data and applications are protected while the user must take measures to reinforce their application and use strong passwords and verification measures. The popularity of “CLOUD" has brought great simplicity 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 an example, consumers in Smart Grid can obtain their energy usage data in a fine-grained manner and are confident to share their personal energy usage data with others . From the collected data a report is created, and one can compare their energy expenditure with others. Due to its openness, data sharing is always deployed in a unfriendly environment and open 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:

Consistency of data: The situation of Smart Grid, the statistic energy usage data being confusing if it is copied by opponents. While this issues alone can be solved using well established cryptographic tools, one may meet additional difficulties when other issues are taken into account, such as secrecy and capacity.
Un singularity :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 secrecy of consumers applications, and any failures to do so may lead to the refusal from the consumers to share data with others.
Effectiveness: The number of users in a data sharing system could be large and a practical system must decrease 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.

II. RELATED WORK

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.An “identity-based ring signature”, is an efficient solution on applications requiring data authenticity and anonymity. 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 defence on signature producer. A user can sign secretly 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.

ID-based ring signature seems to be an best transaction among efficiency, data validity and anonymity, and provides a sound solution on data sharing with a large number of members. To obtain a higher level security, one can add more users in the ring. But doing this increases the chance of key disclosure as well. Key disclosure is the primary limitation of ordinary digital signatures. If the private key of a signer is compromised, all signatures of that signer become insignificant, future signatures are invalidated and no previously issued signatures can be trusted. Once a key outflow 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 concept of forward secure signature was proposed to preserve the validity of past signatures even if the current secret key is compromised.

The issue of key disclosure is more severe in a ring signature scheme: if a ring member’s secret key is exposed, the opponent can produce valid ring signatures of any documents 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 needs to include the compromised user in the “group" of his choice. As a result, the disclosure 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 differentiate 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.

III. PROPOSED SYSTEM

In this paper, increased security in ID-based Ring Signature is projected, which is an essential tool for building time reducing commercial reliable and unsigned data sharing system. Provided formal definitions on forward secure ID-based ring signatures.

- In ID-based setting, the elimination of the expensive certificate confirmation process makes it scalable and especially suitable for big data analytic environment.
- Key update process only requires an exponentiation.

DOI: 10.15680/IJIRCCE.2016.0407149

- The concept of linkable ring signatures are implemented. They are ring signatures, but with added linkability. Such signatures allow anyone to decide if two signatures are signed by the same group member (in which case the two signatures are said to be linked).
- Improved security in uploading data or signing of messages in reduced amount of time and memory.

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

3.1 The Design

The identities and user secret keys are valid in to T periods and make the time intervals public.

Setup

For joining a ring group the user or the data owner has to sign up for the first time. The data centre module then approves the user and he is directed to get a key for further processing .The Public Key Generator module 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

When the user joins a group and the data centre approves him, he can upload or download data to the cloud. For this he has to join a group and request for a key. The pkg module distribute the key on request. 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.

Update

After a specific time interval, the secret key of the user gets expired and for further processing he has to update his key. On inputting the secret key for a time period t, if t<T the user updates the key.

Sign

The user can sign messages on behalf of him after his approval by the data centre module and receiving his secret keys from the public key generator.

Verify

To verify a signature for a message m, a list of identities L and the time period t check all the parameters and the output is valid if all equalities hold, otherwise output invalid.

Opener

The opener module opens the messages signed by the users.

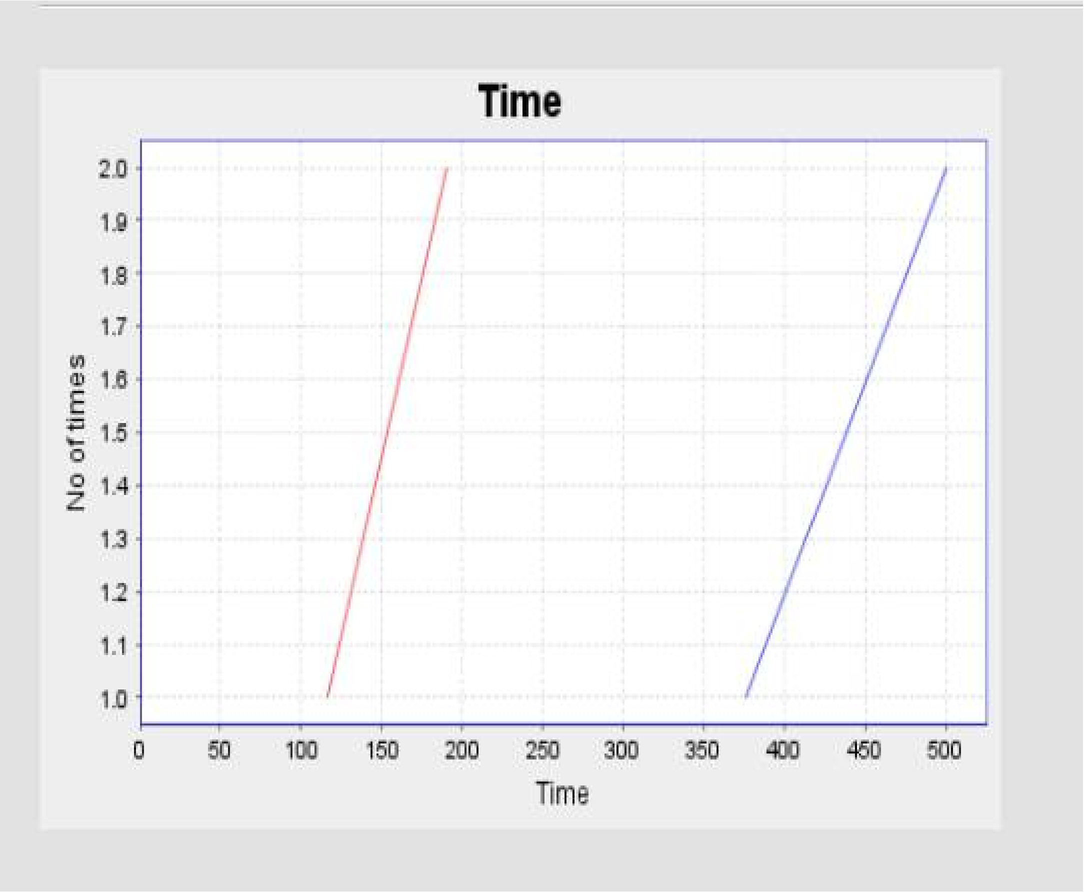
Linker

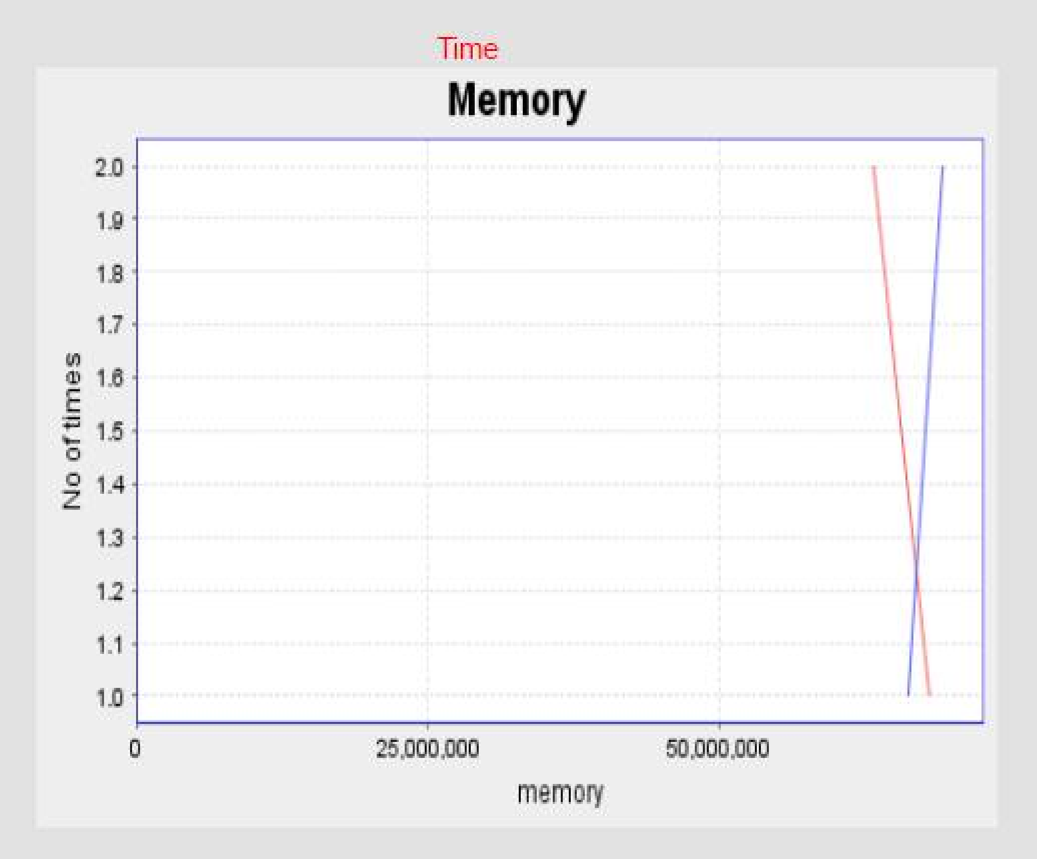
Linkable ring signatures are ring signatures, but with added linkability: such signatures allow anyone to determine if two signatures are signed by the same group member (in which case the two signatures are said to be linked). If a user signs only once on behalf of a group, the user still enjoys secrecy similar to that in conventional ring signature schemes. If the user signs multiple times, anyone can tell that these signatures have been generated by the same group member.

IV. EVALUATION

The performance of this scheme with respect to three entities: the private key generator (PKG) for Increased security, the data owner (user), and the service provider (data centre). In the experiments, the programs for three entities are implemented. All experiments were repeated several times to obtain average results shown in the paper. The results shows that the proposed system is better in performance in both time and memory. Adding forward security can further improve the security protection level. With forward security, the key exposure problem can be solved. This provides a more fair, justice, safety and efficient environment for many business applications.

A number of assessments were done and graphs are plotted on the basis of the results. This shows that that the newly proposed system performs better both in the case of time and memory.





V. Conclusion

Encouraged by the realistic needs in data sharing, a new view called forward secure ID-based ring signature is implemented. It allows an ID-based ring signature scheme to have forward security. The scheme provides total secrecy. Scheme will be very useful in many other practical applications, especially to those require user privacy and authentication. In addition to this with added linkability feature allow anyone to determine if two signatures are signed by the same group member. If a user signs only once on behalf of a group, the user still enjoys secrecy similar to that in conventional ring signature schemes.

References

1. Xinyi Huang, Joseph K. Liu+, " Cost-EffectiveAuthentic 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. 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 requirementsand 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, pp. 431 448.
8. 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. Cryptol. 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 sublinear 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:Avision for socially motivated resource sharing”, IEEE Trans.Serv.Comput.,vol.5,no.4,pp.551–563,FourthQuarter2012.

BIOGRAPHY

Anisha S pursuing M.Tech degree in Computer Science and engineering from Mangalam college of engineering, Mahatma Gandhi university. She received B.Tech degree in 2009 from Ilahia college of engineering, Mahatma Gandhi university, Kottayam, Kerala, India. Her research interest includes relational databases, security etc.

Neethu Mariya John received the M.Tech degree in Computer science & Engineering from Anna University, Chennai, in 2007. In 2007, she joined the Department of Computer Science & Engineering, Viswajyothi college of Engineering & Technology, Vazhakulam where she was an Assistant Professor. In 2010, she joined the Department of Computer Science & Engineering, Mangalam College of Engineering, Ettumanoor, as an Associate Professor. Her current research interests include Computer Architecture and Data Management and Theory of Computation. She is a Life Member of the Indian Society for Technical Education (ISTE).