SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 117–122

ISSN No: 2454-9614

Efficient Data Sharing Forward Security

K.K. Abhijith, V. Anoop*, Jishnu.P.Vijayakumar, V. Vinayak, S. Senthilnathan

Department of Computer Science and Engineering,Sri Venkateswara Hi-tech Engineering College Gobi ,Tamilnadu, India.

*Corresponding Author: K.K.Abhijith

E-mail:abhijithkk4321@gmail.com,

Received: 10/11/2015, Revised: 03/12/2015 and Accepted: 10/03/2016

Abstract

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional Public Key Infrastructure 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 project, we further enhance the security of ID-based ring signature by providing forward security.

Reviewed by **ICETSET'16** *organizing committee*

1. Introduction

The popularity and widespread use of “CLOUD” have 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 plat-form such as Microsoft Home 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 in Smart Grid as an example, there are several security goals a practical sys- tem must meet, including Data Authenticity. In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries. While this issue 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 efficiency; Anonymity. Energy usage data contains vast information of consumers, from which one can extract the number of persons in the home, the types of electric utilities used in a specific time period, etc. Thus, it is critical to protect the anonymity of consumers in such application and any failures to do so may lead to the reluctance from the consumers to share data with others; and Efficiency. The number of users in a data sharing system could be HUGE 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. This paper is devoted to investigating fundamental security tools for realizing the three properties we described. Note that there are other security issues in a data sharing system which are equally important, such as availability

1.1. Identity-Based Ring Signature

The aforementioned three issues remind us a cryptographic primitive "identity-based ring signature", an efficient solution on applications requiring data authenticity and anonymity.

1.2. 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 A private key generator then computes private keys from its master secret for users. This property avoids the need of certificates and associates an implicit public key to each user within 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 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.

2. System Design

After careful analysis the system has been identified to have the following modules:

1. Authentication.
2. Data sharing.
3. Cloud computing.
4. Identity-based Ring Signature.
5. Forward security.
6. Smart grid.

2.1. Authentication

Authentication is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an art effect by carbon dating, or ensuring that a product is what its packaging and labelling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

2.2. Data Sharing

Data sharing is the practice of making data used for scholarly research available to other investigators. Replication has a long history in science. The motto of The Royal Society is 'Nullius in verbal', translated "Take no man's word for it. Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be part of the scientific method. A number of funding agencies and science journals require authors of peer-reviewed papers to share any supplemental information (raw data, statistical methods or source code) necessary to understand develop or reproduce published research. A great deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In the absence of any binding requirement, data sharing is at the discretion of the scientists themselves. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and subject/patient/victim confidentiality. Data sharing may also be restricted to protect institutions and scientists from use of data for political purposes. Data and methods may be requested from an author years after publication. In order to encourage data sharing and prevent the loss or corruption of data, a number of funding agencies and journals established policies on data archiving.

2.3. Cloud Computing

Cloud computing is a computing term or metaphor that evolved in the late 2000s, based on utility and consumption of computer resources. Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud.

2.4. Identity Based Ring Signature

Private or hybrid 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) and associates an implicit public key (user identity) to each user within 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.

2.5. Forward Security

In cryptography, forward secrecy (FS; also known as perfect forward secrecy, or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. 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 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 are 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.

2.6 Smart Grid

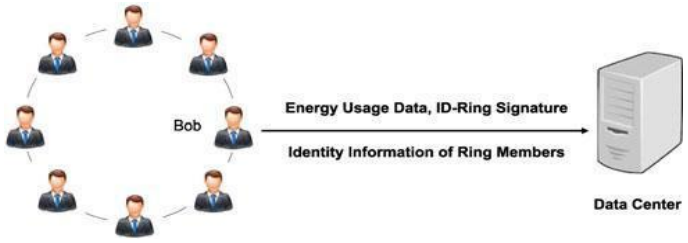
A smart grid is a modernized electrical grid that uses analogue or digital information and communications technology to gather and act on information such as information about the behaviours of suppliers and consumers - in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the We implement the Smart Grid example introduced in Section and evaluate the performance of our IDFSRS scheme with respect to three entities: the private key generator the energy data owner and the service provider 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 jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the PKG to setup the system is shown in Table 4, where the tested 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 jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the data owner (user) to sign energy usage data with different choices of n and T are shown in Fig. 3 and 4, for jNj = 1024 bits and jNj = 2048 bits respectively. The tested for the user is a laptop personal computer equipped with 2.10 GHz Intel.

3. Proposed System Description

Motivated by the practical needs in data sharing, we proposed a new notion called 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 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. We believe our scheme will be very useful in many other practical applications.

4. System Architecture



Due to its natural framework, ring signature in ID-based set-ting has a significant advantage over its counterpart in traditional public key setting, especially in the big data analytic environment. Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 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 in Fig. 2, 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 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 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.

5. Conclusion

Motivated by the practical needs in data sharing, we proposed a new notion called 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 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. 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, "Manuscript, 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, andD. S. Wong, "ID-based ring signature scheme secure in the standard model," in Proc. 1st Int.Workshop Security Adv. Inform Compute Security,2006, vol. 4266, pp. 1–16.

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