IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCRTET-17

National Conference on Recent Trends in Engineering & Technology

Government Polytechnic College Kasaragod, Kerala

Vol. 4, Special Issue 1

Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Seetha Das V

MTech Scholar, Computer Science & Engineering, LBS College of engineering kasaragod, Kerala, India

Abstract: Cloud computing is an internet based computing that provides shared computer processing resources and data to computers and other devices on demand. Data sharing has never been easier and less demanding to the advanced cloud computing, and the correct examination on the information gives a variety of advantages t both the society and people. Data sharing with an extensive number of participants must consider a few issues, includes efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to build an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate the data which can be stored into the cloud or analysis purpose. Identity-based (ID) ring signature is an alternative to traditional public key cryptography, based on infrastructures (PKI). In PKI have a cost consuming certificate verification which is becomes bottleneck for the solution to be scalable. So the ID based ring signature reduces the process of certificate verification.

Key words: authentication, data sharing, cloud computing, forward security

I. INTRODUCTION

The wide use of CLOUD has brought incredible comfort for data sharing and gathering. As a delegate illustration, purchasers in Smart Grid can acquire their vitality use information in a fine- grained way and are supported to impart their own vitality use information to others. From the collected data a report is created, and user can compare their energy consumption with others. Not only can individuals gain useful information all the more effortlessly, sharing information with others can give a number of advantages to our general 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 transferring the information to an outsider stage such as Microsoft Hohm (Fig. 1). From the gathered information a measurable report is made, and one can think about their vitality utilization with others (e.g., from the same square).This ability to access, analyze, and respond to much more accurate and detailed data/information from the levels of the electric grid is critical to efficient for energy usage. Due to its openness, data sharing is always deployed in an unfriendly environment and vulnerable to a number of security threats. In this paper enhance the security of ID-based ring signature by providing forward security. If a secret key of any user has been leaked, all previous generated signatures that include this user still remain valid. Taking energy usage data sharing in Smart Grid as an example, there are several security goals a practical system must meet, includes:

- Data Authenticity: In the circumstance of Smart Grid, the measurement usage of energy data would be misleading. While this issue can be solved using well known cryptographic tools for e.g., message authentication code or digital signatures, one may experience additional troubles at the point when different issues are considered like anonymity and efficiency.
- Anonymity: Energy usage data sharing system contains large information of consumers, from which one can separate the any number of peoples in the home, the types of electric utilities utilized in a specific time period, etc. Thus, it is judicial or 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.
- Efficiency: The quantity of users in a data sharing framework could be LARGE, imagine a smart grid with a country size, and a practical system must reduce the computation and communication cost.

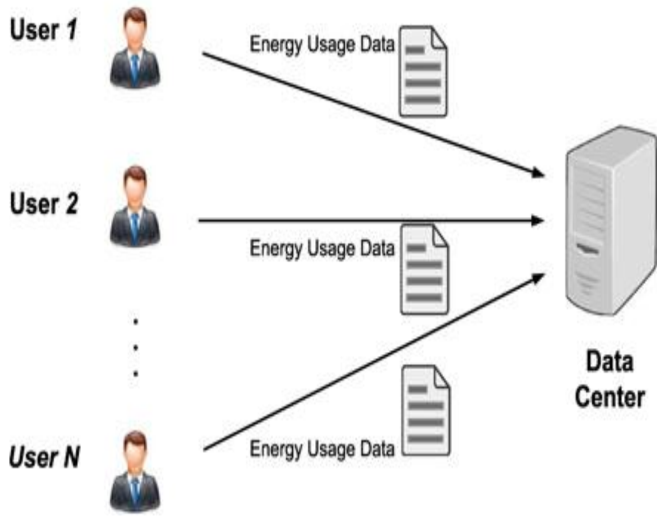

Fig. 1. Energy usage data sharing in smart grid.

1.1 Identity Based Ring Signature

For data authenticity and anonymity identity based ring signature is an efficient solution.

1.1.1 ID based Cryptosystem

The traditional open key cryptosystem requires a trusted Certificate Authority (CA) to issue computerized testaments that tie clients to their open keys. Since the CA needs to create its own signature on every client's open key and deal with every client's declaration. So this is a costly and complex process. To overcome this Identity Based public cryptosystem was used. The ID based cryptosystem first introduced by Shamir. In ID based Cryptosystem public key of every client’s is generated from a string relating to this current clients freely known information’s (e.g.an email address, a private address, and so on). Then the private key generator (PKG) generates private key from its lord mystery for clients. This property will avoid the certificates and distribution of implicit public key to each user with in the system. To check an ID-based signature, different from the traditional public key based signature, one doesn't have to check the certificate first. The elimination of the certificate validation makes the whole verification process more efficient.

1.1.2. Ring signature scheme

In cryptography, a ring signature is a kind of computerized signature that can be performed by any individual from a gathering of clients that each have keys. Along these lines, a message signed with a ring signature is embraced by somebody in a specific gathering of individuals. One of the security properties of a ring signature is that it ought to be computationally infeasible to figure out which of the gathering individuals' keys was utilized to deliver the signature. A user can sign anonymously on behalf of a group on his 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.

1.1.3. Advantage in Big Data

Due to its characteristic structure, ring signature in ID-based setting has a noteworthy preferred over its counterpart in traditional open key setting, especially in the huge data analytic environment. Suppose there are 10,000 clients in the ring, the verifier of a traditional open key based ring signature must first approve 10,000 certificates of the corresponding client's, after which one can carry out the actual verification on the message and signature combine. In difference, to verify an ID-based ring signature, just the identities of ring client's, 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 an extraordinary amount of time and calculation. 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 huge number of clients such as energy data sharing in smart grid:

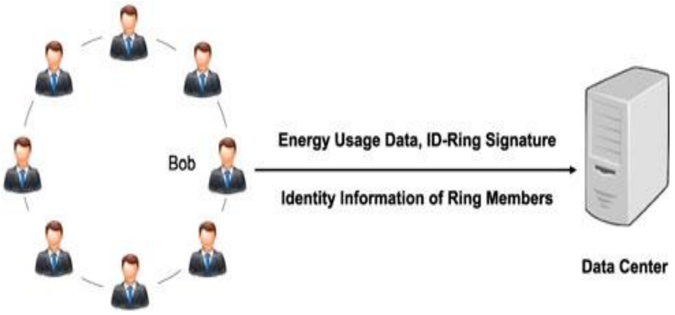
Bob
Energy Usage Data, ID-Ring Signature
Identity Information of Ring Members
Data Center

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

• Step 1: The energy data owner (say, Bob) first setups a ring by picking a gathering of clients. This phase just needs public in general character data of ring individuals, for example, private addresses, and Bob does not require the joint effort (or the assent) from any ring individuals.
• Step 2: Bob uploads his own information of electronic utilization, together with a ring signature and identity information of all ring individuals.
• Step 3: By confirming the ring signature, one can be guaranteed that the information is for sure given out by a valid resident (from the ring individuals) while can't make sense of who the resident is. Henceforth the efficient of the information supplier is guaranteed together with information realness. In the interim, the confirmation is productive which does not include any declaration confirmation.
First ID-based ring signature scheme was proposed was proven secure in the random oracle model. Two constructions in the standard model were proposed. Their first construction however was discovered to be flawed, 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 Han et al. under the trusted setup assumption. However, their proof is wrong and is pointed out by.

1.1.4. Key Exposure

Ordinary digital signatures have a fundamental limitation: If the secret key of a signer is compromised, all the signatures of that signer become worthless. This may become quite a realistic threat since if the secret key is compromised, any message can be forged. All future signatures are invalidated as a result of such a compromise, and more importantly, no previously issued signatures can be trusted. Once a leakage has been identified, there may exists some key revocation mechanism to be involved immediately in order to prevent the generation of any signature using the compromised secret key. However, this does not solve the problem of forge ability for past signatures. It is not possible to ask the signer to re-issue all previous signatures due to many physical and practical limitations. The problem of key exposure in a ring signature scheme is more serious. In ring signature schemes, if a user’s secret key is exposed to an adversary, the adversary can generate not only ordinary digital signature for any documents, but he can also sign any documents on behalf of the group. More badly, the group can be defined by the adversary due to the spontaneity property of ring signature schemes. The exposure of one user’s secret key not only requires changing the public key pairs for the whole group, but also renders all previously obtained ring signatures invalid, because one cannot distinguish whether a signature is generated by an adversary after it has obtained one of the secret keys or by the legitimate user before the adversary got the secret key.
Forward-secure signature schemes are designed to resolve the key exposure fundamental limitation of digital signature. The goal of a forward-secure signature scheme is to preserve the validity of past signatures even if the current secret key has been compromised. Forward security property means that even if the current secret key is compromised, an adversary cannot forge signatures for past time periods. In other words, the forger can only forge signatures for documents pertaining to time periods after the exposure but not before. The integrity of documents signed before the exposure remains intact. The concept of forward security is to reduce the damage of exposure of any secret key of users in ring signature. That is, even when a secret key is compromised, previously generated ring signatures remain valid and do not need to be regenerated.

II. MOTIVATION

Public key cryptography and digital signatures are an important building block of today's computer security. However, the theoretical foundations of their security are quite weak. The whole security relies on unproven assumptions. For high or long term security requirements this is particularly unsatisfying.The RSA algorithm is the most popular asymmetric public key algorithm. It can be used for both signing and encryption..

III. CONTRIBUTION

In this paper propose the method for signature that is RSA, which is the tool for the secure signature based on RSA crypto system.

- We prove the security of the proposed scheme is provably secure
- Our implementation have
  1) It is in ID based setting. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analysis environment.
  2) The size of the secrete key is just one integer.
  3) Key update process only requires an exponentiation
  4) We do not require any pairing in any stages.

IV. CONCLUSION

Motivated by the practical needs in data sharing, introduce 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 unforgeable

REFERENCES

[1]. 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.
[2]. M. Bellare and S. Miner, “A forward-secure digital signature scheme,” in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.
[3]. R. Cramer and V. Shoup, “Signature schemes based on the strong RSA assumption,” in Proc. ACM Conf. Comput. Commun. Security, 1999, pp. 46–51.
[4]. J. Herranz, “Identity-based ring signatures from RSA,” Theor. Comput. Sci., vol. 389, no. 1-2, pp. 100–117, 2007
[5]. A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. CRYPTO 84 Adv. Cryptol., 1984, vol. 196, pp. 47–53.
[6]. Johannes B□ock "RSA-PSS Provably secure RSA Signatures and their Implementation v1.0.3" in This work is licensed under a Creative Commons Attribution 3.0 License.,2011
[7]. http://rsapss.hboeck.de/
[8]. Javier Herranz “Identity-based ring signatures from RSA” in Theoretical Computer Science 389 (2007) 100–117
[9]. Mihir Bellare “A Forward-Secure Digital Signature Scheme” in Advances in Cryptology { Crypto 99 Proceedings.
[10]. Joseph K. Liu “Solutions to Key Exposure Problem in Ring Signature”.