IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Genuine and Incognito Data Sharing with Forward Security

Dr Mohammed Abdul Waheed[1], Maheshwari Rathod[2]

Associate Professor, Dept. of Computer Science and Engineering, VTU RO PG Centre, Kalaburagi, Karnataka, India[1]

PG Student, Department of Computer Science and Engineering, VTU RO PG Centre, Kalaburagi, Karnataka, India[2]

Abstract: With further developments in cloud computing, data sharing has never been easier and a further review on the data sharing provides results which can be advantageous both to the society and individuals. When considering a large number of users, data sharing needs to take into account issues like optimisation, data integrity and secrecy of the data owned. One of the methods to do this is Ring Signature which proves to be promising. The main advantage is that it helps in creating an anonymous and genuine data sharing system. It further provides the owner of the data to anonymously authenticate his/her data which can be further put in cloud for further review later. The disadvantage for the Ring Signature is the expensive certificate verification in the traditional public key infrastructure (PKI). To overcome this disadvantage, Identity-based (ID-based) ring signature can be used which eliminates the process of certificate verification. This paper discusses about enhancing the security of the ID-based ring signature further by providing forward security. Considering a scenario wherein the secret key of a specific user is compromised then what is done is that all the previously generated signatures will still remain valid. By doing this, we eliminate the tedious job of re-authenticating the secret key of the user in question. This proves to be advantageous in cases where there is large scale data sharing. This paper further discusses about increasing the efficiency, security and provides algorithms so as to implement the system and show its practicality.

Keywords: cloud computing, smart grid, Ring signature, Forward Security.

I. INTRODUCTION

The fame and extensive use of "CLOUD" have carried great handiness for data sharing and gathering [8]. Not only can persons obtain helpful data more easily, sharing data with others can give a quantity of profit to our public as well [14].

As a envoy example, clients in Smart Grid can acquire their energy practice data in a fine-grained manner and are habitude to distribute their personal energy usage data with others, e.g., by uploading the information to a third party plat-form such as Microsoft Hohm. From the collected data a statistical description is produced, and one can evaluate their energy usage with others i.e. from the same block.

This skill to access, examine, and reply to much more accurate and full data from all stages of the electric grid is dangerous to well-organized energy usage.Appropriate to its directness, data sharing is at all times organized in an aggressive atmosphere and susceptible to a quantity of security fears. Considering energy utilizing data sharing in Smart Grid as a model, there are numerous security objectives to a practical system must meet, as well as:

1. No corrupt data: In case of smart grid, the energy usage data may be incorrect if it is altered by adversaries. It may be overcome by the cryptographic tools but for other goals like secrecy and efficiency, the existing system proves to be a disadvantage.

2. Secrecy: The energy data contains data about the consumers from which anyone can obtain the number of persons in the home, etc. Therefore it becomes critical to protect the secrecy of users in such applications.

3. Efficiency: In a data sharing system, the number of users can be very large i.e. it can be a smart grid with country size. The practical system should decrease computation and communication cost as much as possible. If this is not done then it would lead to wastage of energy which contradicts the goal of Smart Grid.

II. RELATED WORK

Data Authenticity: In the situation of smart grid, the statistic energy usage data would be misleading if it is forged by adversaries. [1] While this issue alone can be solved using well established cryptographic tools (e.g., message authentication code or digital signatures), 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 applications, and any failures to do so may lead to the reluctance from the consumers to share data with others; Efficiency. [4] The

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

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. Otherwise it would lead to a waste of energy, which contradicts the goal of smart grid[1],[2],[3].

III. PROBLEM STATEMENT

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 signature invalid (if 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.

IV. OBJECTIVE

To enable effective data sharing via clouds by the method of public key infrastructure (PKI) which safe guards the secrecy and integrity of the data. It further provides safe sharing of data to trusted third party users with minimal compromise on data security or reliability.

V. PROPOSED WORK

We propose a new notion called forward secure ID-based ring signature, which is an essential tool for building Cost-effective authentic and anonymous data sharing sys- tem: For the first time, we provide formal definitions on forward secure ID-based ring signatures; I present a concrete design of forward secure ID- based ring signature. No previous ID-based ring signature schemes in the literature have the property of for- ward security, and we are the first to provide this feature; I prove the security of the proposed scheme in the random oracle model, under the standard RSA assumption.

Advantages :

- It is 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.
- We do not require any pairing in any stage.

1. Algorithm for RSA

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

1. Key Generation

I. Choose two distinct prime numbers p and q.

II. Find n such that n = p q. n will be used as the modulus for both the public and private keys.

III. Find the totient of n, (n) (n) = (p-1)(q-1).

IV. Choose an e such that 1 ¡ e ¡ (n), and such that e and (n) share no divisors other than 1 (e and (n) are relatively Prime). e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation de 1 (mod (n)).

In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or (n). This is often computed using the Extended Euclidean Algorithm, since e and (n) are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent.

The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption

1) Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.
2) When Person B wishes to send the message "M" to Person A, he first converts M to an integer such that 0 ¡ m ¡ n by using agreed upon reversible protocol known as a padding scheme.
3) Person B computes, with Person A's public key information, the cipher text corresponding to c me (mod n).
4) Person B now sends message"M" in cipher text, or c, to Person A.

3. Decryption

1) Person A recovers m from c by using his/her private key exponent, d, by the computation m cd (mod n).
2) Given m, Person A can recover the original message"M" by reversing the padding scheme.

2. Our proposed ID-Forward Secure Scheme Ring Signature Scheme

ID-based forward secure ring signature scheme are designed to following ways. The identities and user secret keys are valid into T periods and makes the time intervals public and also set the message space M= { 0,1 }*.

Sign: On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set L = {IDi ∈ {0, 1}∗|i ∈ [1, n]} of n user identities, a message m ∈ M, and a secret key sk π,t ∈ D, π ∈ [1, n] for time period t, the algorithm outputs a signature σ ∈ Ψ.

Verify: On input a list param of system parameters, a time period t, a group size n of length polynomial in λ, a set L = {IDi ∈ {0, 1}∗|i ∈ [1, n]} of n user identities, a message m ∈ M, a signature σ ∈ Ψ, it outputs either valid or invalid.

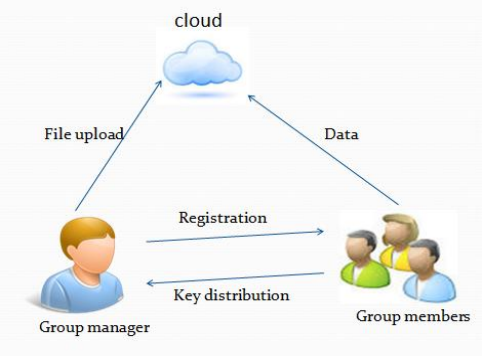
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Update: On input a user secret key ski,t for a time period t, the algorithm outputs a new user secret key ski,t+1 for the time period t + 1.

VI. SYSTEM ARCHITECTURE



The above figure illustrates the main theme of group manager and group members.

1) Group members register with the group manager.
2) Group manager then sends Private key to all group members.
3) Group manager then uploads the data to cloud; later this same data can be retrieved from cloud by the group members.

VII. CONCLUSION

Inspired by the realistic requirements in data sharing, we proposed a new idea called forward secure ID-based ring signature. It permits an ID-based ring signature scheme to have advanced security. It is the first in the literature to have this characteristic for ring signature in ID-based setting. Our system affords unconditional secrecy and can be verified forward security. Our idea is very well-organized and does not require any pairing operations. The size of client secret key is just one integer, while the key update process just needs an exponentiation. We consider our system will be very useful in many other realistic applications, particularly to those needed user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. Our present scheme relies to show the security. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work.

ACKNOWLEDGEMENT

We would like to take this opportunity to express my sincere gratitude to my Project Guide **Dr. Mohammed Abdul Waheed** (Associate Professor, Computer Science and Engineering Department) for his encouragement, guidance, and insight throughout the research and in the preparation of this dissertation.

He truly exemplifies the merit of technical excellence and academic wisdom.

REFERENCES

[1]. Xinyi Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security", IEEE TRANSACTIONS ON COMPUTERS VOL: 64 NO: 6 YEAR 2015

[2]. 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.

[3]. 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.

[4]. 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.

[5]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. "Privacypreserving public auditing for secure cloud storage". IEEE Trans.Computers, 62(2):362–375, 2013.

[6]. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n Signatures from a Variety of Keys. In ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 415–432. Springer, 2002.

[7]. 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.

[8]. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 255–270. Springer, 2000.

[9]. 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.

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