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. 3, Issue 11, November 2015

Authentic Cloud Data Sharing and Data Security Using Trusted Third Party

Keda Shivaji Pawar, Sandip.A.Kahate

M.E Student, Dept. of Computer Engineering, Sharadchandra Pawar College of Engineering, Dumbarwadi, Otur, Maharastra, India

Assistance Professor, Dept. of C.E., SharadchandraPawar College of Engineering, Dumbarwadi, Otur, Maharastra,India

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 (PKI) 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. I further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of one single user has been compromised. I provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality. The TTP module receives encrypted file F from the data owner and computes hash value H(F) using SHA-1 algorithm. It stores H(F) in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). TTP send file F to CSP module to store on cloud.

KEYWORDS: Trusted Third Party, Cloud Service Provider, Ring signature, Authentication, data sharing, cloud computing, forward security, smart grid.

I. 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 ex-ample, 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 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 in Smart Grid as an example, there are several security goals a practical system 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 (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; and Efficiency. The number of users in a data sharing sys- tem 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.

DOI: 10.15680/IJIRCCE.2015. 0311134

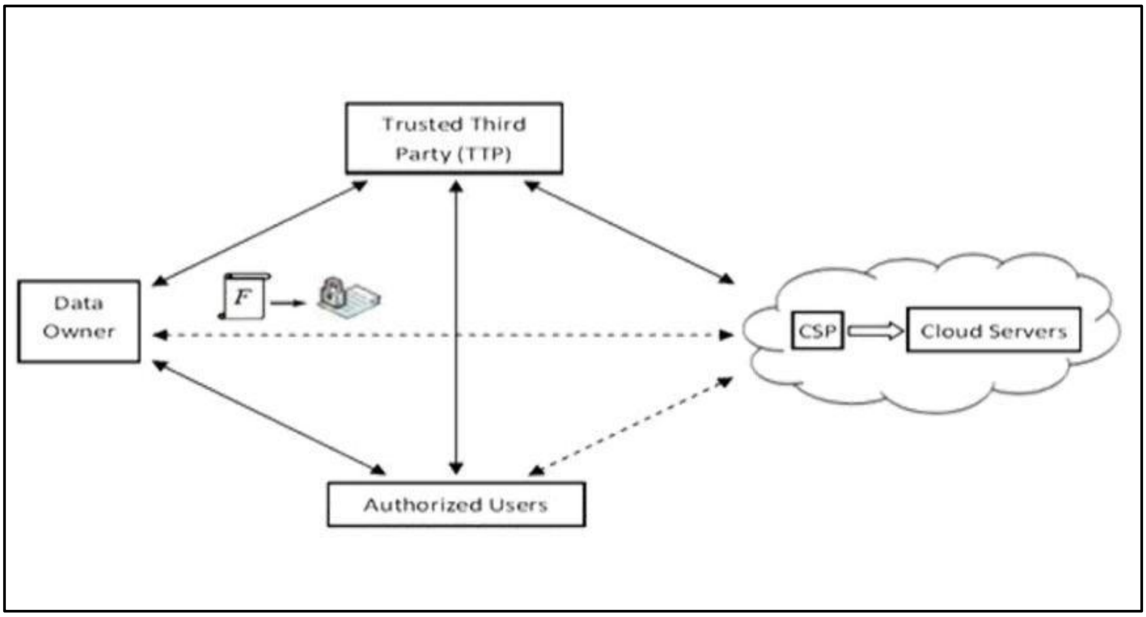
II. RELATED WORK

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 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. PROPOSED ALGORITHM

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; and implementation is practical, in the following ways:

1) 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.
2) The size of a secret key is just one integer.
3) Key update process only requires an exponentiation.
4) We do not require any pairing in any stage.



Trusted Third Party / Auditor

Database auditing involves a database to not be unaware of the actions of the database users. Database administrators and consultants frequently set up auditing for the security purposes. For example to ensure that advice to be accessed by those without the permission do not access it. Auditing is the monitoring and recording of user database activities thatare selected. It might be based on combinations of variables that can include user name, program, time, and so on, including the kind of SQL statement executed, or on individual activities. Auditing can be triggered by security policies when specified components including, within an Oracle database are obtained or altered the contents within a given object. Auditing is usually used to:Enable future responsibility for current actions affecting unique content, or taken in a certain schema, table, or row. Deter users (or others) from improper actions according to that answerability.Inquire questionable action For example; if some user is deleting data then the security administrator might decide to audit all connections to all successful and unsuccessful deletions of rows and the database from all tables in the database. Notify an auditor the user has more privileges than expected which can lead to reassessing user authorizations and an unauthorized user deleting or is manipulating information. Screen and assemble information about database activities that are specific o For example, the database administrator can collect data about which tables are being upgraded, how many logical I/Os are performed, or how many concurrent users connect at peak times. Find issues with an authorization or access control execution.

Authorized User:-Authorized User is a client of owner who has right to access the remote data.

Cloud Storage Service Provider (CSP):-Database is provided by cloud Storage Services Provider. It permits information owner to keep any kind of information and also able to make the user define database schema. It can be Non SQL / SQL form of database instance. According to user requirement CSP will allocated the space for the user instance

IV. PSEUDO CODE

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

I. Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.
II. 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.
III. Person B computes, with Person A’s public key information, the cipher text corresponding to c me (mod n).
IV. Person B now sends message ”M” in cipher text, or c, to Person A.

3. Decryption

I. Person A recovers m from c by using his/her private key exponent, d, by the computation m cd (mod n).
II. Given m, Person A can recover the original message ”M” by reversing the padding scheme.
This procedure works since.

c me (mod n), cd (me)d (mod n), cd mde (mod n). By the symmetry
property mods we have that mdemde (mod n).
Since de = 1 + k(n), we can write
mde m1 + k(n) (mod n), mde m(mk)(n) (mod n), mde m (mod n).
From Euler's Theorem and the Chinese Remainder Theorem, we can show that this is true for all m and the original message.
cd m (mod n), is obtained.

V. ACKNOWLEDGEMENT

We would like to take this opportunity to express my sincere gratitude to my Project GuideProf.S.A.Kahate (Assistant Professor, Computer 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.

VI. CONCLUSION AND FUTURE WORK

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.

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.