IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 36-39
www.iosrjournals.org

New Approach for ID-Based Data Sharing Mechanism with Forward Security

Are Akshay sunil[1], Davange Mayuri Bhausaheb[2], Dhage Diksha Nivrutti[3], Kalwane Ganesh Kaduba[4] M/S. Kale M.N[5]
(Department of Information Technology, Padmashri Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar (MS), India)

Abstract: *With the advancement in the cloud computing data sharing has never been easier, as well as An array of benefits to both the society and individuals provided by the shared data accurate analysis. When there is data sharing with a large number of participants on cloud several issues might considered, these issues may include efficiency, data integrity and also privacy of data owner by the system constructor To construct an anonymous as well as authentic data sharing system to the constructer is promised by the ring signature. Data owners data can be anonymously authenticate by itself, this data can be put into the cloud for storage or for analysis purpose allowed by it. Certificate verification process in the traditional public key infrastructure setting is more costly process. This process may turn to a bottleneck instead for this solution to be scalable. The need for certificate verification process eliminated by the ID-based) group(ring) signature.*

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

I. Introduction

For data sharing and collection use of cloud technology have brought great convenience. Representative ex- consumers in Smart Grid able to obtain their energy usage data in a fine-grained manner as well as they are encouraged to share their personal energy usage data with others, e.g., by uploading the data to a TTP(third party platform) e.g. Microsoft Hohm,For efficient energy usage this ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical. Because of its openness, Always data sharing is deployed in a hostile environment as well as vulnerable to a number of security threats. Consider as an example energy usage data sharing in Smart Grid, a practical system must meet several security goals, including:

Data Authenticity- In the situation of smart grid, if data is forged by adversaries then the statistic energy usage data would be misleading. Using well established cryptographic tools (e.g., message authentication code or digital signatures) this issue can be solved , one may encounter additional difficulties when other issues(such as anonymity and efficiency) are taken into account;

Anonymity- Energy usage data contains information of consumers may vast information, from which one able to extract the number of persons in the home, the types of electric utilities used in a specific time period, etc.

Thus, In such applications it is critical to protect the anonymity of consumers, and any failures to do so may lead to the reluctance from the consumers to share data with others;

Efficiency- In a data sharing system the number of users may be HUGE (imagine a smart grid with a country size), and a practical system should reduce the computation and communication cost as much as possible. Otherwise it would lead to a wastage of energy, that will contradicts the goal of smart grid.

1.1 Objectives :

Mainly there are three objectives for our system listed below
•Secure And Confidential data sharing system
•Attribute Based Accessed
•User Authentication at TTP(Trusted Third Party)

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.

III. System Architecture

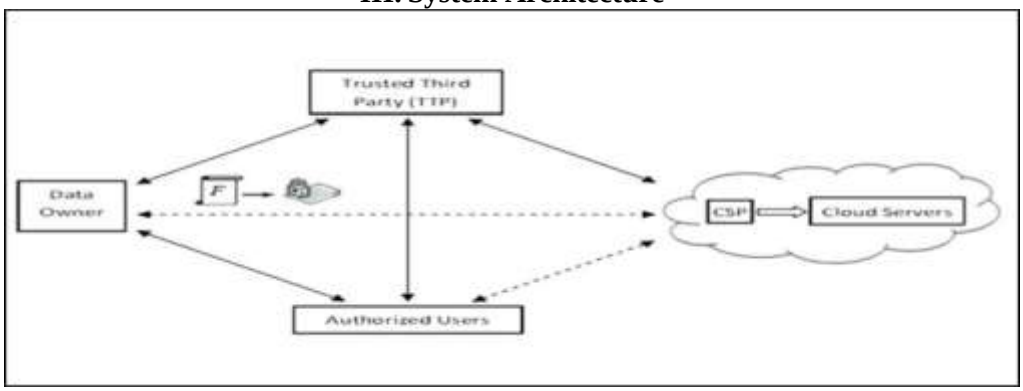

Figure. 3.1 System Architecture

Above fig 3.1 shows the system components and relationship between them.

3.1. Data Owner

Information Owner of the device component is the nothing the user of desire to save and share data over cloud. Information owner isn't having any idea where my information will be stored by the CSP and there is trust shortfall on CSP. As data is most important for info owner and the data owner do not desire that his information is observable to the CSP. To fix the preceding issue set trustworthy third party and before uploading the data, it's encrypted / auditor which are set to keep watch.

3.2. Trusted Third Party

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 that are 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:

1) Enable future responsibility for current actions affecting unique content, or taken in a certain schema, table, or row.

2) Data user (or others) from improper actions according to that answerability.

3) 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.

4) 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.

5) Screen and assemble information about database activities that are specific. For example, the database administrator can collect data about which tables are being up- graded, how many logical I/Os are performed, or how many concurrent users connect at peak times.

6) Find issues with an authorization or access control execution.

3.3 Authorized User

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

3.4cloud 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. Algorithm

Wrapper Encryption Scheme (With two ciphers Text) It consists of key generation, encryption, and decryption algorithms as follows:

4.1 Key Generation:-

The key generator works as follows:

1) 'X' generates an efficient description of a multiplicative cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.

2) 'X' chooses a random *x* from
{1, ..., q-1}.

3) 'X' computes $h=g^x$.

4) 'X' publishes *h*, along with the description of *G,q,g* as her public key. 'X' retains *x* as her private key which must be kept secret.

4.2 Encryption The following is the encryption algorithm to encrypt a message *m* to 'X' under her public key *(G, g, q, h)*

1. 'Y' chooses a random y from {1, …, q-1}, then calculates $C_1=g^y$.
2. 'Y' calculates the shared secret $s=h^y$.
3. 'Y' converts his secret message into an element *m* of *G*.
4. 'Y' calculates $C_2=m.s$
5. 'Y' sends the cipher text $(C_1,C_2) = (g^y,m,(g^x)^y)$ to 'X'.

4.4 Decryption:-

The following is the decryption algorithm to decrypt a cipher text (C_1,C_2) with her private key *x*

1) 'X' calculates the shared secret $s=C_1^x$

2) And then computes $m=C_2.s^{-1}$ which she then converts back into the plaintext message m, where *m* inverse of *s* in the group *G*.

The decryption algorithm produces the intended message, since

$$c_2.s^{-1} = m.h^y.(g^{xy})^{-1} = m.g^{xy}.g^{-xy} = m \quad .$$

V. Conclusion and Future Work

By considering the practical needs in data sharing. we proposed a new notion forward secure ID- based ring signature. This structure ID-based ring signature scheme allows forward security. To have this feature for ring signature in ID-based setting it is first in literature. Our scheme can be proven forward secure unforgivable in the random oracle model the running cost of key generation ,key update ,signing and verifying algorithm log square of the total no. of time period.to share media content in a controllable manner along with provides unconditional anonymity.

Acknowledgment

We would like to take this opportunity to express my sincere gratitude to my Project Guide (Assistant Prof. M/S. M.N.Kale 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
[4]. theory". IEEE Transactions on Information Theory, 57(7):4833–4842, 2011.
[5]. 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
[6]. With different levels of anonymity (extended abstract)". In ProvSec, volume 6402 of Lecture Notes in Computer Science, pages 166– 183. Springer, 2010.
[7]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. "Privacypreserving public auditing for secure cloud storage". IEEE Trans.
[8]. Computers, 62(2):362–375, 2013.