Forward Secure Identity Based Ring Signature for Data Sharing in the Cloud

Bindumol V S
M.Tech. Student
Department of Computer Sciences
School of Computer Sciences Mahatma Gandhi University

Dr.Varghese Paul
Associate Professor
Department of Information Technology
CUSAT

Shyni S T
Assistant Professor
Department of Computer Sciences
School of Computer Sciences Mahatma Gandhi University

Abstract

Cloud Computing is ceaseless growing latest technology in IT industry, academia and business. The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is highly accessible, flexible technology that puts hardware, software, and virtualized resources. Cloud computing infrastructure works over the internet on demand basis. Main features of cloud computing is that on-demand capabilities, broad network access, resource pooling, rapid elasticity ,measured service scalability and provides shared services to user on demand basis in distributed environment. Commonly available cloud computing service providers are Google, Yahoo, Microsoft, Amazon etc. The details of cloud services are abstracted from users. The most common issues of cloud computing as efficiency, integrity and authenticity. Moreover, users are unaware of location where machines which actually process and host their data. The motivation of this paper is to propose a secure data accessing and sharing scheme, for public clouds.
Keywords: Authentication, Data Sharing, Cloud Computing, Forward Security

I. INTRODUCTION

Forward secure identity based ring signature for data sharing in the cloud provide secure data sharing within the group in an efficient manner. It also provide the authenticity and anonymity of the users. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to secretly authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be avoid costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-based ring signature which eliminates the process of certificate verification, can be used instead. The security of ID-based ring signature by providing forward security: If a secret key of any user has been rev, all previous generated signatures that include this user still remain valid. The 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 conceded. Accountability and privacy issues regarding cloud are becoming a significant barrier to the wide adoption of cloud services. There is a lot of advancement takes place in the system with respect to the internet as a major concern in its implementation in a well effective manner respectively and also provide the system in multi-cloud environment. Many of the users are getting attracted to this technology due to the services involved in it followed by the reduced computation followed by the cost and also the reliable data transmission takes place in the system in a well effective manner respectively. The key features are:

A. Data Authenticity:

In a cryptographic sense, authenticity indicates that a message was endorsed by a particular principal. This principal may endorse multiple messages, and the same authentication tag can validate distinct messages. In a data flow sense, authenticity guarantees the provenance of a message, but it does not distinguish between different messages from the same principal. A mere authenticity check does not protect against replay attacks: a message that was authentic in a previous run of the protocol is still authentic

B. Anonymity:

Anonymous communication allows users to send messages to each other without revealing their identity. It is aimed at hiding who performs some action, whereas full privacy requires additionally hiding what actions are being performed. In the context of distributed computation, anonymity allows hiding which users hold which local inputs, whereas privacy requires hiding all information about the inputs except what follows from the outputs.

C. 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 securing transactions online transactions typically require: message integrity to ensure messages are unaltered during transit message confidentiality to ensure message content remain secret non-repudiation to ensure that the sending party cannot deny sending the received message and sender authentication to prove sender identity.

II. RELATED WORK

An exhaustive literature survey has been conducted to identify related research works conducted in this area. Abstracts of some of the most relevant research works are included below.

A. Identity-based Ring Signature

Javier Herranz IIIA, "Identity-Based Ring Signatures from RSA" Artificial Intelligence Research Institute, CSIC, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain

Identity-predicated (ID-predicated) cryptosystems eliminate the desideratum for validity checking of the certificates and the desideratum for registering for a certificate afore getting the public key. These two features are desirable especially for the efficiency and the authentic spontaneity of ring signature, where a utilizer can anonymously sign a message on behalf of a group of spontaneously conscripted users including the authentic signer. The identity-predicated ring signature and distributed ring signature schemes, involve many public keys, it is especially intriguing to consider an identity-predicated construction which evades the management of many digital certificates. The first that is distributed ring signature schemes for identity-predicated scenarios which do not employ bilinear pairings. A paramount property of the scheme is additionally formally presented and analyzed: opening the anonymity of a signature is possible when the authentic author wants to do so. The security of all the considered schemes can be formally proved in the desultory oracle model. The security of ID-predicated signature schemes is formalized by considering the most vigorous possible kind of attacks: culled messages/identities attacks.

- Ring structure formation for data sharing.
- Eliminate the costly certificate verification.

B. Forward-Secure Digital Signature Scheme

MihirBellare and Sara K. Miner "A Forward-Secure Digital Signature Scheme" Dept. of Computer Science, & Engineering University of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA

Digital signature scheme in which the public key is fine-tuned but the secret signing key is updated at customary intervals so as to provide forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be utilizable to mitigate the damage caused by key exposure without requiring distribution of keys. The construction uses conceptions from the signature schemes, and is proven to be forward secure predicated on the hardness of factoring, in the arbitrary oracle model. The construction is additionally quite efficient.

Past signature remain secure even if expose the current secret key.

C. Security and Privacy-Enhancing Multicloud Architectures

Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And Privacy-Enhancing Multicloud Architectures" Member, IEEE, Luigi Lo Iacono

Security challenges are still among the most astronomically immense obstacles when considering the adoption of cloud accommodations. This triggered a plethora of research activities, resulting in a quantity of proposals targeting the sundry cloud security threats. The conception of making utilization of multiple clouds has been distinguishing the following architectural patterns: Replication of applications sanctions to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the utilizer to get evidence on the integrity of the result. Partition of application System into tiers sanctions disuniting the logic from the data. This gives adscititious aegis against data leakage due to imperfections in the application logic. Partition of application logic into fragments sanctions distributing the application logic to distinct clouds. This has two benefits. First no cloud provider learns the consummate application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality. Partition of application data into fragments sanctions distributing fine-grained fragments of the data to distinct clouds. The fundamental underlying conception is to utilize multiple distinct clouds at the same time to mitigate the jeopardies of maleficent data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust postulation can be lowered to a postulation of non-collaborating cloud accommodation providers. Further, this setting makes it much harder for an external assailant to retrieve or tamper hosted data or applications of a concrete cloud utilizer. These approaches are operating on different cloud accommodation levels, are partly amalgamated with cryptographic methods, and targeting different utilization scenarios.

- Data sharing in multi-cloud environment.
- Data security in multi-cloud.

III. SYSTEM ARCHITECTURE

Forward secure identity predicated ring signature for data sharing in the cloud architecture that proposed data sharing in an efficient manner. This architecture, provide multiple cloud environment for astronomically immense data sharing in secure way. Client in the diagram represents individual cloud accommodation utilizer. The servers may reside in different physical locations. The CSP decides the servers to store the data depending upon available spaces. Identity predicated ring signature provide the ring formation of users. The authentic data sharing in multiple clouds to provide secure data sharing at sizably voluminous system. The encryption and decryption provide secure data transmission

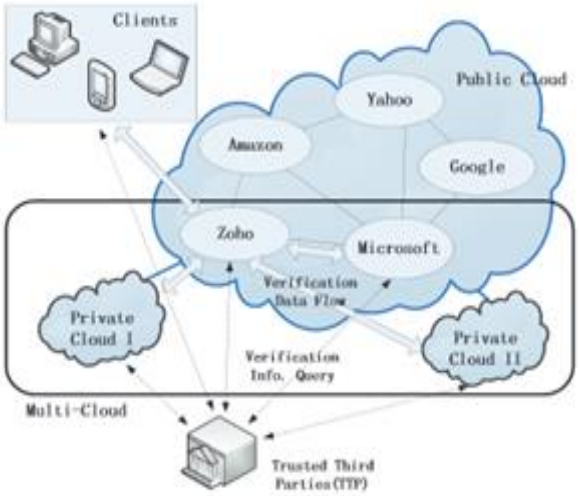

Fig. 1: System Architecture

IV. IMPLEMENTATION

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 }*.

A. Setup:

On input of a security parameter λ, the PKGgenerates two random k-bit prime numbers p and q such that p = 2p′ +1 and q = 2q′ +1 where p′, q′ are some primes. It computes N = p*q. For some fixed parameter it chooses a random prime number e such that $2^{\ell} < e < 2^{\ell+1}$ and gcd (e,∅(N)) = 1. It chooses two hash functions H1 :{0,1}*→ ZN* andH2 : {0,1}*→{0,1}. The public parameters param are (k,l,e,N,H1,H2) and the master secret key msk is (p, q).

B. Extract:

For user i, where i∈ Z, with identity IDi∈{0,1}* requests for a secret key at time period (denoted by an integer), where 0 ≤t < T, the PKG computes the user secret key using its knowledge of the factorization of N.

$$sk_{i,t} = [H_1(ID_i)]^{\frac{1}{e^{(T+1-t)}}} \bmod N$$

C. Update:

On input a secret key sk i,t for a time period t, if t < T the user updates the secret key as otherwise the algorithm outputs meaning that the secret key has expired.

D. Sign:

To sign a message m ∈{0,1}* in time period t, where 0 ≤t < T, on behalf of a ring of identities L = {ID1,….,IDn}, a user with identity IDπ ∈ Land secret key skπ,t:

1) For all i∈{1,…,n},i ≠π, choose random Ai∈Z*N and compute

$$R_i = A_i^{e^{(T+1-t)}} \bmod N \text{ and } h_i = H_2(\mathcal{L}, m, t, ID_i, R_i)$$

2) Choose random Aπ ∈Z*N and compute

$$R_\pi = A_\pi^{e^{(T+1-t)}} \cdot \prod_{i=1, i\neq\pi}^{n} H_1(ID_i)^{-h_i} \bmod N$$

$$h_\pi = H_2(\mathcal{L}, m, t, ID_\pi, R_\pi)$$

3) Compute s= (skπ,t)hπ.$\prod_{i=1}^{n} A_i \bmod N$
4) Output the signature for the list of identities L, the message m, and the time period t as

σ=(R1,…,Rn,h1,…,hn,s).

E. Verify:

To verify a signature $\sigma$for a message m, a list tf identities L and the time period t, check whether hi = H2 (L,m,t,IDi,Ri) for i= 1,…, n and

$$s^{e^{(T+1-t)}} = \prod_{i=1}^{n} \left(R_i \cdot H_1(ID_i)^{h_i}\right) \bmod N$$

Output valid if all equalities hold otherwise output invalid

V. CONCLUSIONS AND FUTURE ENHANCEMENT

The Forward Secure ID-Predicated Ring Signature sanctions an ID-predicated ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. The scheme provides unconditional anonymity and can be proven forward-secure unforgeable in the desultory oracle model. The scheme is very efficient and does not require any pairing operations. The size of utilizer secret key is just one integer, while the key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially to those require utilizer privacy and authentication, such as ad-hoc network, e-commerce activities and perspicacious grid. The system withal implemented in multi-cloud system to ameliorate the efficiency, sizably voluminous storage and data sharing system. Thus Reduce computation involution of designation and verify. Reduce space and time requisites ameliorate the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation to prove its security. Consider a provably secure scheme with the same features in the standard model as an open quandary and our future research work

REFERENCES

[1] Huang, Joseph K. Liu+, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou "Cost-effective authentic and anonymous data sharing with forward security".DOI:10.1109/TC.2014.2315619,IEEE Transactions on Computers.
[2] Javier Herranz IIIA, " Identity-Based Ring Signatures From RSA " Artificial Intelligence Research Institute, CSIC, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain
[3] MihirBellare and Sara K. Miner" A Forward-Secure Digital Signature Scheme" Dept. of Computer Scienc e, &EngineeringUniversity of California at San Diego, 9500 Gilman Drive La Jolla, CA 92093, USA.
[4] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And Privacy-Enhancing Multicloud Architectures" Member, IEEE,Luigi Lo Iacono.
[5] Gene ItkisBoston University Computer Science Dept.111 Cumming ton St.Boston, "Forward security: Adaptive cryptography-time evolution"MA 02215, USAitkis@bu.edu
[6] Y. Wu, Z. Wei, and R. H. Deng." Attribute-based access to scalable media in cloud-assisted content sharing networks" .IEEE Transactions on Multimedia, 15(4):778–788, 2013.
[7] A. Shamir. "Identity-Based Cryptosystems and Signature Schemes".In CRYPTO 1984, volume 196 of Lecture Notes in Computer Science,pages 47–53. Springer, 1999.
[8] D. S. Wong, K. Fung, J. K. Liu, and V. K. Wei. "On the RS-CodeConstruction of Ring Signature Schemes and a Threshold Settingof RST". In ICICS, volume 2836 of Lecture Notes in Computer Science,pages 34–46. Springer, 2003.
[9] 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.
[10] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen. Forward- secure identity-based signature: Security notions and construc- tion. Inf. Sci., 181(3):648–660, 2011.
[11] H. Xiong, Z. Qin, and F. Li. An anonymous sealed-bid electronic auction based on ring signature. I. J. Network Security, 8(3):235– 242, 2009.
[12] W. Susilo, Y. Mu, and F. Zhang. Perfect Concurrent Signature Schemes. In ICICS 2004, volume 3269 of Lecture Notes in Computer Science, pages 14–26. Springer, Oct. 2004.
[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy- preserving public auditing for secure cloud storage. IEEE Trans. Computers, 62(2):362–375, 2013.
[14] G. Yan, D. Wen, S. Olariu, and M. Weigle. Security challenges in vehicular cloud computing. IEEE Trans. Intelligent Transportation Systems, 14(1):284–294, 2013.