ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Cost Effective Authentic and Anonymous Data Sharing With Forward Security

Shreyas S. Barde, Rupa R. Kandule, Laxmi R. Salunke, Prof. Ashok Kumar.

Department of Computer Engineering, G.S. Moze College of Engineering, Balewadi, Pune, MH, 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. In this paper, we 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. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

I. INTRODUCTION

Forward secure character based ring signature for data sharing in the cloud provide secure data sharing of within the group in an efficient manner. It also provide of the authenticity and anonymity of the users. Ring signature is the promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to thein secret authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be to avoid costly certificate verification in the traditional public key infrastructure setting becomes a bottleneck for this solution to be scalable. Identity-based ring the signature which is eliminates of the process of certificate for verification can be used instead. The security of the ID-based ring signature by providing forward security: If a secret key of any user has been revolution, all previous generated signatures that include this user still remain valid. The property is especially important to any large scale of data sharing system, as it is impossible to ask all data owners to re-authenticate their data even if a secret key of the one single user has been conceded. Accountability and privacy issues regarding cloud are becoming the significant barrier to the wide adoption of cloud services. There is the lot of advancement takes place in the system with respect to the internet as a major concern in it'simplementation in a well effective manner respectively and also provide of the system in multi-cloud environment. Many of the users are a getting attracted to this technology due to the services involved in it the followed by the reduced computation followed by the cost and also the reliable data of transmission takes place in the system in a well effective manner respectively.[9]

Research Background:

A. Data Authenticity:

In a cryptographic sense, the authenticity indicates that the message was endorsed by the particular principal. This principal may endorse multiple messages, and of the same authentication tag can be validate distinct messages. In an data flow sense, authenticity guarantees the provenance of the message, but it does not the distinguish between different messages from the same principal. A mere authenticity check does not protect against replay attacks: the message that was authentic in a previous run of the protocol is still authentic [10]

B. **Anonymity:**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Anonymous communication allows users to send messages to each other without revealing of their identity. It is the aimed at hiding who performs some action, whereas full privacy requires additionally hiding what are actions are being performed. In the context of distributed computation, anonymity allows hiding which users hold which local inputs, whereas privacy requires hiding all the information about the inputs except what follows from the outputs [10]

C. **Efficiency:**
The number of users in a data sharing system could be huge and a practical system must reduce of the computation and communication cost as much as possible securing transactions online transactions typically require: message integrity to the ensure messages are unaltered during transit message confidentiality to ensure message content remains secret non-repudiation to the ensure that the sending party cannot deny sending the received message and sender authentication to the prove sender identity.

II. LITERATURE REVIEW

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

1. **Identity-based Ring Signature:**
Javier Herranz IIIA, "Identity-Based Ring Signatures from RSA" Artificial Intelligence Research Institute, Spanish National Research Council, Campus UAB s/n, E-08193 Bellaterra, Spain Identity-predicated cryptosystems eliminate the desideratum for validity checking of the certificates and the desideratum for registering for a certificate afor getting the public key. These two features are desirable especially for the efficiency and the authentic spontaneity of the ring signature, where a utilizer can anonymously sign a message on behalf of a group of spontaneously conscripted users includingof 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.
2. **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.
3. **Security and Privacy-Enhancing Multicloud Architectures:**
Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security And the Privacy-Enhancing Multicloud Architectures" Member, IEEE, Luigi Lo Iacono Security challenges are still among of the most astronomically immense obstacles when considering the adoption of cloud accommodations. This triggered a plethora of research activities, resulting in the quantity of proposals targeting the sundry cloud security threats. The conception of making utilization of the multiple clouds has been distinguishing the following architectural patterns: Replication of applications sanctions to the receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables of the utilizer to get evidence on the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

integrity of the result. Partition of application System into the tiers sanctions disuniting the logic from the data. This gives adscititious aegis against data leakage due to the imperfections in the application logic. Partition of application logic into fragments sanctions distributing the application logic to the distinct clouds. This has two benefits. First no cloud provider learns the consummate application logic. Second, no cloud provider learns to the overall calculated result of the application. Thus, this leads to the data and application confidentiality. Partition of the application data into fragments sanctions distributing fine-grained fragments of the data to the distinct clouds. These approaches are operating on different cloud accommodation levels, are the partly amalgamated with cryptographic methods, and the targeting different utilization scenarios.

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

III. CONCLUSION AND FUTURE WORK

The Forward Secure ID-Predicated Ring Signature sanctions an ID-predicated ring signature scheme have forward to security. It is the first in the literature to have this feature for ring signature in ID-predicated setting. The scheme provides of 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 a key update process only requires an exponentiation. This will be very utilizable in many other practical applications, especially tothe those require utilizer privacy and authentication, such as ad-hoc network, e-commerce of activities and perspicacious grid. The system withal implemented in multi-cloud system tothe ameliorate the efficiency sizably voluminous storage and data sharing system. Thus Reduce computation involution of designation and verify. Reduce of space and time requisites ameliorate the cost efficient mechanism. The current scheme relies on the arbitrary oracle postulation tothe prove its security. Consider a provably secure scheme with the same features in the standard model as an open for quandary and our future research work.

REFERENCES

1. IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013 “Attribute-Based Access to Scalable Media inCloud-Assisted Content Sharing Networks by theYongdong Wu, Zhuo Wei, and Robert H. Deng.
2. New Generic Constructions and Their Applications”Forward-Secure Identity Based Signature: New Generic Constructions and Their Applications”
3. University of the Wollongong Research Online “Improvements on an authentication scheme for vehicular sensor networks” Liu, J. K., Yuen, T. Hon., Au, M. & Susilo, W. (2014).
4. Liu, J. K., Au, M., Huang, X., Susilo, W., Zhou, J. & Yu, Y. (2014). New insight to a preserve online survey accuracy and privacy in bigdata era. Lecture Notes in Computer Science, 8713 (PART 2), 182-199.
5. International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012”Distributed Accountability for Data Sharing in Cloud.
6. IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 7, NO. 3, JULY-SEPTEMBER 2014“ASocial Compute Cloud: Allocating and the SharingInfrastructure Resources via Social Networks.
7. International Journal of Advance Research in theComputer Science and Management Studies
“Secure Data Sharing in Cloud for Distributed Accountability using Patchy Image Encryption.
8. IOSR Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 69-72 “PRIVACY & DATA INTEGRITY FOR THE SECURE CLOUD STORAGE.
9. IJSTE - International Journal of Science Technology & Engineering “Forward Secure Identity Based Signature for Data Sharing in the Cloud by Bindumal V.S ,Dr.Varghese Paul,Shyni S.T.
10. International Journal of Innovative Research in Computerand Communication Engineering”A Comparative Study on Privacy-PreservingPublic Auditing for the Secure Cloud Storage by Vikram.J1, M.Kalimuthu2 PG Scholar, Department of Information Technology, SNS College of Technology, Coimbatore, Tamil Nadu, India1.Associate Professor, Department of Information Technology, Coimbatore Tamil Nadu.