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

Anonymous Data Security using Ring Topology in Cloud: A Survey

Archana Shelke, Prof. Prashant Joshi

Dept. of Computer Engineering & Technology, GHRIET, , Savitribai Phule Pune University, Pune, India

ABSTRACT: Cloud Computing is unending growing latest technology in IT industry, academia and business. The practice of using a network of remote servers introduced on the internet to store, manage, and process data, rather than a local server or a personal computer. Cloud computing is the highly accessible, flexible technology that puts hardware, software, and virtualized resources. Cloud computing substructure works over the internet on demand basis. Main features of cloud computing is that on-demand capabilities, broad network access, resource sharing, rapid elasticity ,measured service scalability and provides shared services to user on demand basis in the distributed environment. In the cloud computing most common issues are such as efficiency, integrity and authenticity. Moreover, users are ignorant of location where machines which actually process and host of their data. The motivation behind this paper is to propose a secure data reading and sharing scheme, for public clouds.

I.INTRODUCTION

Cloud computing service providers such as Google, Yahoo, Microsoft, etc abstracts the detailed cloud services from users. Secured data sharing using forward secure character based ring signature in the cloud provides data sharing within the group in an efficient manner. It also provides the authenticity and anonymity of the users. Ring signature is the promising way to construct an anonymous and authentic data sharing system. It allows a data owner to provide security to authenticate his data which can be put into the cloud for storage or analysis purpose. The system can be used to avoid costly certificate verification in the traditional public key infrastructure setting which becomes a bottleneck for this solution to be scalable. Instead of that Identity-based ring signature which eliminates the process of certificate for verification. 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 its implementation 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]

II.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]

DOI: 10.15680/IJIRCCE.2015. 0311253

B. **Anonymity:**

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.

III.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 a for 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 including of 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:**

Mihir Bellare 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 secured 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 Multi cloud Architectures:**

Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, "Security and the Privacy-Enhancing Multi cloud 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 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 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 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.

IV.EXISTING APPROACHES

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 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.

V.PROPOSED SYSTEM

1. System Architecture

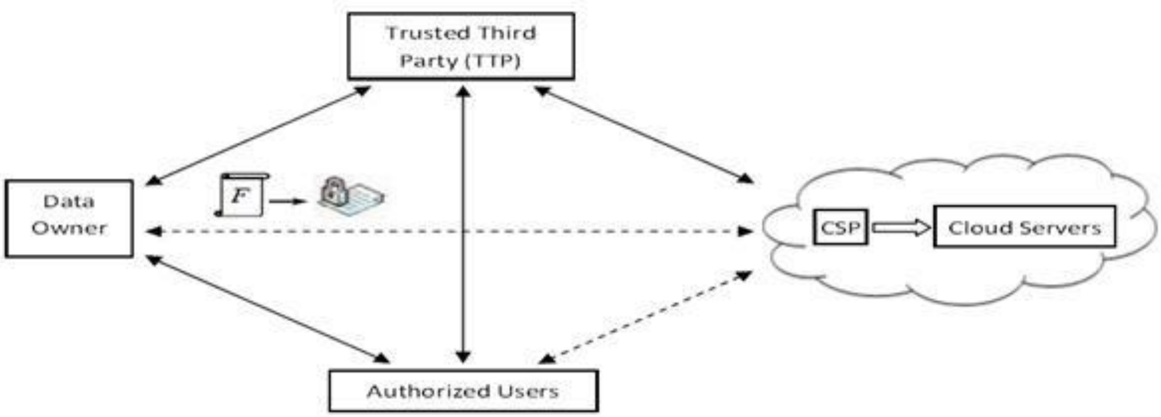

Figure 1: Cloud computing data storage system model

Above figure shows the system components and relationship between them.

- **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.

- **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 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 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.

VI.CONCLUSION AND FUTURE WORK

The Forward Secure ID-Predicated Ring Signature sanctions an ID-predicated ring signature scheme has forward 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 unforgivable 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 to those require utilizer privacy and authentication, such as ad-hoc network, e-commerce of activities and perspicacious grid. The system with implemented in multi-cloud system to the 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 to the 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] 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] 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

[3] M. Bellare and S. Miner, "A forward-secure digital signature scheme," in Proc. 19th Annu. Int. Cryptol. Conf., 1999, vol. 1666, pp. 431–448.

[4] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, Security and privacy-enhancing multicloud architectures," IEEE Trans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224, Jul. \Aug. 2013.

[5] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in Proc. 8th Int. Conf. Theory Appl. Cryptol. Inform. Security: Adv. Cryptol., 2002, vol. 2501, pp. 415–432.

[6] 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.)

[7] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, “A practical and provably secure coalition-resistant group signature scheme,” in Proc. 20th Annu. Int. Cryptol. Conf. Adv. Cryptol., 2000, vol. 1880, pp. 255–270.

[8] M. H. Au, J. K. Liu, T. H. Yuen, and D. S. Wong, “ID-based ring signature scheme secure in the standard model,” in Proc. 1st Int. Workshop Security Adv. Inform. Comput. Security, 2006, vol. 4266, pp. 1–16.

[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

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

[12] M. Bellare, D. Micciancio, and B. Warinschi, “Foundations of group signatures: Formal definitions, simplified requirements and a construction based on general assumptions,” in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Techn., 2003, vol. 2656, pp. 614–629.

[13]International Journal of Innovative Research in Computerand Communication Engineering”A Comparative Study on Privacy-Preserving Public 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.

[14]IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013 “Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks by theYongdong Wu, Zhuo Wei, and Robert H. Deng.

[15]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.

[16]International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012”Distributed Accountability for Data Sharing in Cloud.