International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

Effective Anonymous Data Sharing with Forward Security in Cloud - A Survey

Mary Vidya John[1], G. Keerthana[2], Giridharan R.[3], J. Suchith Samuel[4], Mitali M. Javkar[5]

[1]Asst. professor, [2,3,4,5]UG Students
Dept. of Computer Science and Engineering, Vemana Institute of Technology,
Koramangala, Bangalore-560034, Karnataka, India

Abstract* - *The advancements in cloud computing has made data sharing easier. Data sharing with multiple users must consider several issues, including efficiency, data integrity and privacy of data owner. Ring signature enables data owners to anonymously authenticate their data and upload into the cloud for storage or analysis purpose. The costly certificate verification in the public key infrastructure (PKI) is eliminated by using Identity-based (ID-based) ring signature with forward security: If a secret key of any user has been compromised, all previously generated signatures that include the user remain valid. Forward security 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.

Keywords* - *Cloud Computing, Forward Security, Ring Signature

I. INTRODUCTION

Cloud is a platform that enables a user to access and use services provided by it. Cloud computing makes storing and processing of data easier either on a privately-owned data center or on a third-party data centre. Cloud storage refers to a hosted object storage service, but it is bound to include other types of data as well. Cloud computing is based on sharing of resources to achieve the quality of being logical and consistent. To make sharing of data efficient in a group we use ring signature which is a type of digital signature that can be done by any of the members of the group where each member in the group is provided with keys. Files are usually targeted files such as PDF's, word processor documents, spreadsheets. Ring signature is the promising candidate to construct an anonymous and authentic data sharing system. Ring signature alone cannot provide security for data sharing so we use a new scheme called forward security: if the current secret key of a user has been compromised the previously generated signatures by the user remain valid [1].Forward Security is very important to any large scale data sharing system, as it is impossible to ask data owners to reauthenticate their data.

Document sharing services in the cloud allow users to share and collaborate on files and documents. Data sharing in the cloud is vulnerable to many privacy and security attacks. There are several security goals that data sharing system must meet, including. Data Authenticity: The process of confirming the origin and integrity of data is called data authentication. In group users the data being shared would be deceiving in case if it is formed by foes. While this issue alone can be fathomed utilizing settled cryptographic apparatus (e.g., ring signature), one may encounter additional inconveniences exactly when diverse issues are viewed as, for example, obscurity and proficiency. Data authentication has two elements: authenticating that you're getting data from the correct entity and validating the integrity of that data. Anonymity: In some situations, it is necessary to hide the identity of the users and the operations being performed by the user. Anonymous data sharing decreases the chances of the identity being revealed hence increasing the security of the user. It is fundamental to guarantee the secrecy of users in anonymous data sharing applications, and any failure to do all these things considered may incite the reluctance from the members of the group to give information to others. Efficiency: The data sharing system can contain a large number of users. It is necessary for an efficient data sharing system to reduce the computation cost and time as much as possible failing to do so would lead to waste of energy. Data integrity: It is important to ensure that the data sent remain unaltered during the transit of the message. It is also important to keep the contents of the message secret by which the receiver can be sure that the correct data is received. Figure 1 illustrates the main roles of group manager and group members: Group members register with the group manager. Group manager then sends Private key to all group members. Group manager is responsible for uploading data of the group users to cloud; later this same data can be retrieved from cloud by group members.

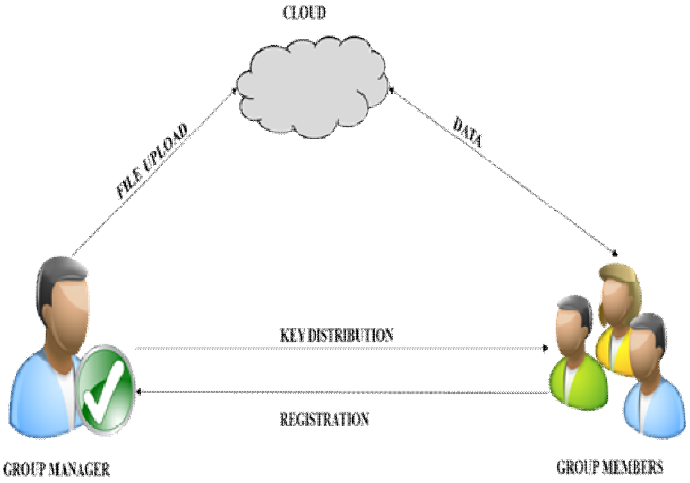

Figure 1: System architecture showing Interaction of group manager and members

II. LITERATURE SURVEY

A. Ring Signature

In cryptography [2], any member of a group of users, each having keys, can perform a ring signature which is a type of digital signature. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. The two-difficult task in group formation is computational cost and encryption techniques which are overcome by ring signature. The group manager plays a vital role in group formation. The computationally infeasible property to determine which of the group member's keys was used to produce the signature makes ring signature efficiently secure. The disadvantages of attribute-based encryption, dynamic broadcast encryption, and group signature have been overcome by ring signature. Ring signatures and group signature differ in the following ways: first, there is no way to revoke the anonymity of an individual signature, and second, without additional setup, any group of users can be used as a group. Ring signature obtained its name from the ring-like structure of the signature algorithm. The ring signature schemes with the sub-linear size of the signature, as well as with constant size are efficient.

B. Forward Security

Forward Security [3] also known as Forward Secrecy is a property of secure communication protocols in which the long-term keys are not compromised and it protects sessions against intrusion by Secret Keys (or) Passwords. Motivated by the practical needs in data sharing, proposal of a new notation called Forward Secure ID based Ring Signature came into existence. It allows an ID – Base Ring Signature scheme to have Forward Security. Forward Security is a necessary requirement that a big data sharing system requires, otherwise it will lead to huge waste of time and resource. Forward secure signature scheme is, first of all, a key-evolving signature scheme. It consists of four algorithms: a key generation algorithm, a key update algorithm, a signature algorithm and a verification algorithm termed into FSIG.key, FSIG.update, FSIG.sign and FSIG. Verify where:

1. **FSIG.key**: the key generation algorithm, is a probabilistic algorithm which takes as input a security parameter and total number of time periods, and generates a Public Key and the Initial Secret Key.
2. **FSIG.update:** the key update algorithm is a probabilistic algorithm which takes as input the Secret Key of the current period, and generates the new Secret Key for the next period.
3. **FSIG.sign**: the signature algorithm, takes as input the Secret Key, of the current time-period and a message, and generates a signature for that period. This algorithm may be probabilistic.
4. **FSIG.verify**: the verification algorithm, is a deterministic algorithm which takes as input the Public Key, a message and a candidate signature, and output when there is either a valid signature or not.

A Public-Key system has the property of Forward Security if it generates one random Secret Key per session to complete key agreement, without using a deterministic algorithm. This means the intrusion of one message cannot cause intrusion of others as well, and there is no secret value whose acquisition would compromise multiple messages. Together with Forward Security, there is also anonymity which serves as the notations of security. Therefore, Forward Security enhances the protection of all entities.

C. Group formation in the cloud

Cloud storage is a new business solution for remote backup outsourcing, as it offers infinite storage space for clients. Cloud storage helps enterprises and government organizations to significantly reduce the financial overhead of data management, since they can archive their data remotely to third-party cloud storage providers instead of maintaining data center on their own Security is considered to be the most important aspect of cloud computing environment due to the critical information stored in the cloud.

The main aim of cloud security is focused on the problems related to data security and privacy aspects in cloud computing. The approach storing of metadata in private cloud prevents the unauthorized retrieval of data by hackers and intruders. Three common cloud service layers (IaaS, PaaS, SaaS) share the commonality in public cloud that is end users digital assets are taken from intra organization to inter organizational context. Parallel usage of multiple clouds can be used to minimize risk and data applications in public cloud. The two major important issues related to user data are privacy preservation and data integrity. Data is saved on an autonomous business party in cloud and it contributes data storage.

D. Data sharing in cloud

Data sharing [4] is the ability to share same data resource with multiple users at a particular instance. It implies that the multiple applications or users. It implies that the data are stored in one or more servers in the network and there is a software locking mechanism that prevents data from being changed by two people at the same time. Cloud storage has become a cornerstone for many businesses. It has become important to create the necessary tools that will effectively protect user's data from access from unauthorized resources. Sharing data between multiple users under the same domain in a secure and efficient way is highly significant. Since Cloud-based services are ideal for businesses, it is necessary to add a level of flexibility and agility that can give businesses a real advantage over competitors. Ensuring that stored data are protected at all times in order to avoid outages and protect data from breaches and certain threats is a non trivial problem. The Cloud stores Data in the cloud and shares multiple users, who can modify the shared data as a group. To ensure data sharing has integrity, users in the group need signature on all data blocks. When a shared data is being created by a user, each and every user in the particular group can have permission to access and to have the appropriate permissions to alter the data.

III. PROBLEM DEFINITION

The number of users in data sharing system could be huge, and a practical system must reduce the computation and communication cost as much as possible. The other issue of secure data sharing is key exposure which is more rigorous in a ring signature scheme: if a ring member's secret key is exposed, the adversary can produce valid ring signatures of any documents on behalf of that group. Thus, the exposure of one user's secret key renders all previously obtained ring signature invalid (if user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. This will lead to a huge waste of time and resource. Hence, the computational cost and encryption techniques were the two major concerns in group formation.

IV. EXISTING SYSTEM

Identity-based(ID-based) cryptosystem, introduced by Shamir eliminated the need of verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID-based cryptosystem, the public key of user is easily computable from a string. A private key generator computes private keys from its master secret for users. This property avoids need of certification. If current key is compromised, then the previously sent data will be considered as invalid. The first ID-based ring signature had been proven secure in the random oracle model. In the standard model, two constructions were proposed. Their first construction, however, was discovered to be flawed, while the second construction is only proven secure in a weaker model, namely, selective-ID model. To obtain a higher-level protection one can add more users in the ring but when we do this it increases the chance of key exposure as well. The fundamental limitation of ordinary digital signatures is key exposure. If the private key of a user is compromised, all signatures of that user become worthless, meaning, future signatures are invalidated and no previously issues signatures can be trusted.

V. PROPOSED SYSTEM

A new scheme called forward secure ID-based ring signature is proposed. It is an essential tool for building Effective anonymous data sharing system with Forward Security. To overcome the flaws in the existing system we use the concept of Forward Security, if current key is compromised then previously generated keys remains valid. The security of the proposed scheme in the random oracle model, under the standard RSA assumption can be proven. Forward Security is a necessary requirement that a big data sharing system requires, to prevent huge waste of time and resource. Formal definitions on forward secure ID-based ring signatures are provided. The elimination of costly verification process makes it scalable and makes it suitable for big data analytic environment. Forward Security therefore, empowers the data sharing capability in terms of Anonymity, Efficiency, Data Authenticity, Availability(service is provided at an acceptable level) and access control (only eligible users can have access to the data). The implementation is practical in following ways:

1. *The size of key is just one integer.*
2. *The update process is just exponentiation.*
3. *we don't require any pairing in any stage.*

VI. CONCLUSION

Motivated by the needs of data sharing a new notion called "Effective Data Sharing with Forward Security" is introduced. From this scheme, we understand that the size of key is just one integer and update process requires exponent. This scheme is very efficient and does not require any pairing operations. Constructing an efficient forward secure signature scheme is still an interesting problem. We believe this scheme will be very useful in many practical applications especially to those which require user privacy and authentication. This can be considered as a provably secure scheme and is an open issue and kept as future explanation work.

ACKNOWLEDGMENT

The authors sincerely thank the Principal, Vemana Institute of Technology for his encouragement and motivation. The authors express their deepest sense of gratitude to Dr. M. Ramakrishna, HoD of Computer Science and Engineering for his constant support and encouragement.

REFERENCES

[1] Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zohu, "Cost effective authentic and anonymous data sharing with forward security".
[2] Dhivya H., Anandakumar H., Sivakumar M., "An effective group formation in the cloud based on ring signature".
[3] Jia Yu, Fanyu Kong, Xiangguo Cheng, Guowen Li, Rong Hao, Xuliang Li, "Security Analysis of a Flexible Forward-Secure Signature Scheme".
[4] Balasaraswathi V.R., Manikandan S., "Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach".

