A Framework for Enhancing Security, Data Sharing and Group Communication in Cloud Platform

Kiruthikaa K V[1], Suresh V[2]
[1, 2] Computer Science and Engineering
[1, 2] Bannari Amman Institute of Technology

Abstract- *Data sharing is one of the most important properties of cloud computing. It enables multiple users to store and share large volume of data in cloud. The major issue that threatens the cloud storage is its security. The root cause for this notable issue is due to cloud openness. There are various security tools and techniques that provide solutions to cloud security. In this paper, the proposed system facilitates an enhanced security technique that combines the features of key management using Identity-based (ID)-based ring signature with forward secrecy. The system also eliminates the process of certificate verification, thereby reducing the communication cost and computation cost*

Keywords- Cloud security, Data sharing, Forward secrecy, Group communication, Identity based ring signature.

I. INTRODUCTION

With the advancement of cloud storage solutions, data sharing among vast group of individuals has now become very easier. Cloud storage offers infinite storage space for clients and also provides new business solutions that support remote backup outsourcing. It significantly reduces the financial overhead of data storage and data management required by various public and private organizations, since they can pile up their data remotely to third-party cloud storage providers instead of maintaining data centers on their own. Security is considered to be the most important aspect of cloud computing environment due to the critical information stored and shared in the cloud. Enhancing cloud security provides integrity, authentication and availability of data to the trusted users of cloud.

II. LITERATURE SURVEY

M. Abe, M. Ohkubo et al.[1] proposed a 1-out-of-n signature from a variety of keys scheme. An oblivious signature with n keys (or messages) is a signature that the recipient can choose one of n keys (or messages) to get signed while the signer cannot find out on which key (or message) the recipient has got the signature. This kind of signature is firstly introduced by L. Chen in 1994. However, the previous reference does not crisply formalize the notion. Furthermore, the proposed constructions are less efficient in both communication and computation.

K. Awasthi and S. Lal [4] described ID-based ring signature and proxy ring signature schemes from bilinear pairings. In a proxy signature scheme, a potential signer delegates his signing power to a proxy, who signs a message on behalf of the original signer. The ring signature allows a user from a set of possible signers to convince the verifier that the author of the signature belongs to the set but identity of the author is not disclosed.

M. Bellare and S. Miner[6] suggested a forward-secure digital signature scheme. A digital signature scheme in which the public key is fixed but the secret signing key is updated at regular intervals so as to provide a forward security property: compromise of the current secret key does not enable an adversary to forge signatures pertaining to the past. This can be useful to mitigate the damage caused by key exposure without requiring distribution of keys.

A. Boldyreva[8] proposed an efficient threshold signature, multi signature and blind signature schemes based on the gap Diffie-Hellman group signature scheme .A robust proactive threshold signature scheme, a multi signature scheme and a blind signature scheme which work in any Gap Diffie-Hellman (GDH) group (where the Computational Diffie-Hellman problem is hard but the Decisional Diffie-Hellman problem is easy). Their constructions are based on the recently proposed GDH signature scheme of Boneh et al.. Due to the instrumental structure of GDH groups and of the base scheme, it turns out that most of our constructions are simpler, more efficient and have more useful properties than similar existing constructions.

J. Herranz[24] suggested identity-based ring signatures from RSA. Identity-based (from now on, denoted also as ID-based) cryptography was introduced by Shamir in 1984 as an alternative to traditional public key cryptography, based on infrastructures (PKI). In PKI-based cryptography, each user generates on his own his secret and public keys. A certification authority must sign a digital certificate which links the identity of the user and his public key. The validity of this certificate must be checked before using the public key of the user, when encrypting a message to him or verifying a signature from him. Obviously, the management of digital certificates decreases the efficiency of practical implementations of public key cryptosystems.

G. Ateniese, J. Camenisch et al.[2]proposed a practical and provably secure coalition-resistant group signature scheme. A group signature scheme allows a group member to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature's originator can be revealed only by a designated entity. The interactive counterparts of group signatures are identity escrow schemes or group identification scheme with revocable anonymity. This work introduces a new provably secure group signature and a companion identity escrow scheme that are significantly more efficient than the state of the art. In its interactive, identity escrow form, our scheme is proven secure and coalition-resistant under the strong RSA and the decisional Hellman assumptions. The security of the non-interactive variant, i.e., the group signature scheme, relies additionally on the Fiat-Shamir heuristic.

M. Li, S. Yu et al [27] described scalable and secure sharing of personal health records in cloud computing using attribute-based encryption technique. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. This paper proposes a novel patient-centric frame work and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, they leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. The paper also focuses on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

Y. Dodis, A. Kiayias et al.[21] described Anonymous Identification in Ad HocGroups .Anonymous identification is an oxymoron with many useful applications. Consider the setting, for a known user population and a known set of resources, where a user wants to gain access to a certain resource. In many cases, accessing the resource is an action that does not mandate positive identification of the user. Instead, it would be sufficient for the user to prove that he belongs to the subset of the population that is supposed to have access to the resource. This would allow the user to lawfully access the resource while protect his real identity and thus “anonymously identify” himself. Given the close relationships between identification schemes and digital signatures, one can easily extend the above reasoning to settings where a user produces a signature that is “signer-ambiguous” i.e., such that the verifier is not capable of distinguishing the actual signer among a subgroup of potential signers. In fact ,it was in the digital signature setting that such an anonymous scheme was presented for the first time; with the introduction of the group signature model which additionally mandates the presence of a designated party able to reveal the identity of the signer, were the need to arise.

D. Boneh, X. Boyen et al.[9] proposed a short group signatures. Signatures in our scheme are approximately the size of a standard RSA signature with the same security. Security of our group signature is based on the Strong Diffie-Hellman assumption and a new assumption in bilinear groups called the Decision Linear assumption.

J.M. Bohli, N. Gruschka et al.[7] stated security and privacy-enhancing multi-cloud architectures. Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third party ,on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software. Clouds can be categorized taking the physical location from the viewpoint of the user into account. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise usually in the own data center this setup is called private cloud. A hybrid approach is denoted as hybrid cloud. This paper will concentrate on public clouds, because these services demand for the highest security requirements

III. PROBLEM DEFINITION

In a large scale cloud data sharing system, the certificate verification process increases the computation cost and communication cost. Computation cost is the cost required generating and updating the keys for all members within a group and communication cost is the cost required to distribute the keys to every member within a group. During group communication, there is an overhead in managing both the group key and secret keys as group membership varies over time when the users enter and leave the group. It ensures that only members of a secure group can gain access to group data and can authenticate group data stored in cloud. It is difficult to re-authenticate the secret keys of all the users, if any single user's secret key is compromised. In such hostile environment, ring signature can be used 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.

IV. PROPOSED SYSTEM

Let us assume a scenario where clients are grouped as a ring like architecture and hence, to provide anonymity and authenticity of shared data in cloud, ring signature is used. Using this security feature, if a secret key of any user has been compromised, then 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. Data sharing with a large number of participants must take into account several issues including efficiency, data integrity and privacy of data owner.

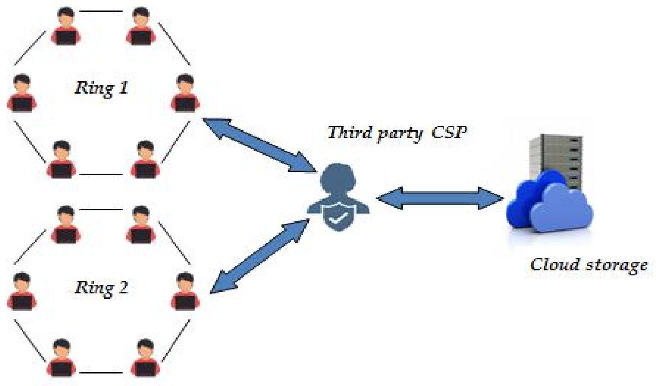

Figure 1. System Architecture

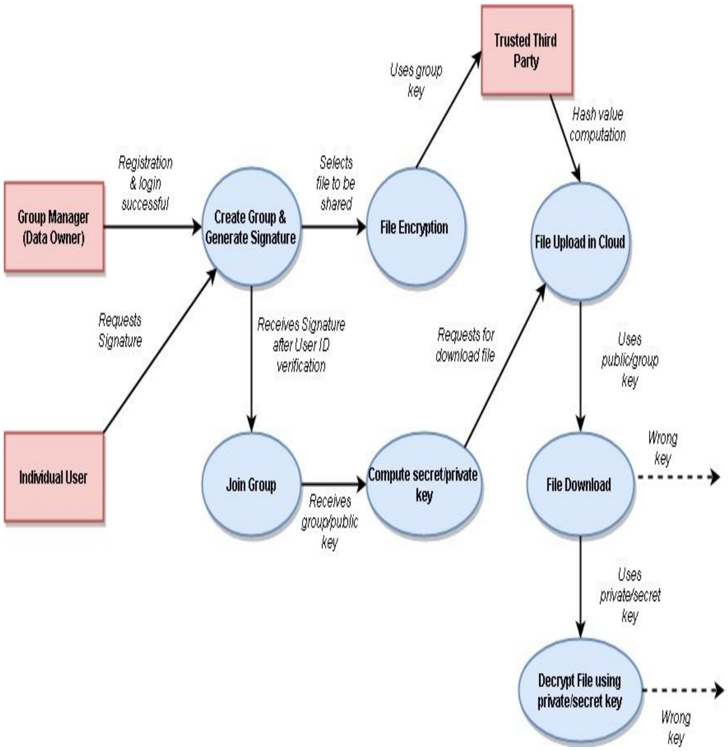
Trusted Third Party
Uses group key
Hash value computation
Group Manager (Data Owner)
Registration & login successful
Create Group & Generate Signature
Selects file to be shared
File Encryption
File Upload in Cloud
Requests Signature
Receives Signature after User ID verification
Requests for download file
Uses public/group key
Individual User
Join Group
Receives group/public key
Compute secret/private key
File Download
Wrong key
Uses private/secret key
Decrypt File using private/secret key
Wrong key

Figure 2. Process of data sharing and group communication

The system architecture shown in Figure 1 comprises of variety of users grouped as ring network. In this system structure, any user of the group can be the owner of the data to be shared, which assures the anonymity property of data sharing in cloud. Besides the advantages of ring signature, the proposed system makes use of ID-based ring signature which further enhances the cloud security along with forward secrecy technique to share and store data in cloud using group key and secret keys.

With forward secrecy, if a secret key of any user has been compromised, then all the previously generated signatures and keys still remain valid. Only the user whose secret key/signature is comprised cannot gain access to the shared data in the group. 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. The system also eliminates the process of certificate verification. The public key of any user is inferred directly from his identity such as e-mail address, telephone number, etc. Later, the user contacts a master entity who uses some secret information to compute the secret key.

Figure 2 depicts the data flow across the proposed system architecture. The owner of the data to be shared in cloud is considered as the group manager. After successful registration, the group manager creates the group i.e., he can decide to whom his data must be shared. The group manager then selects the file or information to be shared among the group that he created.

For secured data sharing, the group manager generates an ID-based ring signature with enabled forward secrecy and also a group or public key. Using the group key, the manager encrypts his file to be shared and send that encrypted file to a trusted third party cloud service provider.

Other individual users also register their identity by providing necessary details. Those users who wish to join the group can send request to the group manager asking for the signature. The group manager acknowledges the user to join his group by sending the signature after verifying the user's identity. Once the individual user joins the group, he receives the group key information which is necessary to compute his secret or private key.

The trusted third party cloud service provider receives the encrypted file or information from the group manager for cloud storage. The third party also verifies the authentication credentials of the group manager and the integrity of the encrypted file. The security of the encrypted file is further enhanced by computing and attaching a secret hash value. Finally, the file is uploaded in cloud database server by the third party.

The group members who wish to view or edit the shared encrypted file sends request to the trusted third party. Since the group members are already verified by the group manager and also possessing the group key, there is no need for the third party to execute the process of certificate verification.

The third party immediately acknowledges the group members by sending the hash key value. The download link of the encrypted file will be available to those having both the group key and hash key values. After downloading the shared file, the group members can decrypt the file using their secret key.

V. CONCLUSION AND FUTURE WORK

The proposed system eliminates the unauthorized access of files and information that is being stored in the cloud using ID-based ring signature with forward secrecy. The communication cost and computation cost will be reduced since group manager does not need to re-authenticate and distribute the group keys each time, whenever a single user's secret key is compromised.

The proposed system illustrates a single file upload in a single cloud database server through a single trusted third party cloud service provider. As a future work, the system can be further modified by uploading multiple files to multiple cloud servers through multiple trusted third parties. In such environment, the users can select and decrypt the files they want to view or edit. Also, the group membership of an individual user is not limited to one particular group.

REFERENCES

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

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

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

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

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

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

[7] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, 2013 "Security and privacy-enhancing multi-cloud architectures," IEEETrans. Dependable Sec. Comput., vol. 10, no. 4, pp. 212–224.

[8] Boldyreva, 2003, "Efficient threshold signature, multi signature and blind signature schemes based on the gap Diffie-Hellman group signature scheme," in Proc. 6th Int. Workshop Theory Practice Public Key Cryptography: Public Key Cryptography ,vol. 567, pp. 31–46.

[9] D. Boneh, X. Boyen, and H. Shacham, 2004, "Short

group signatures," in Proc.Annu.Int. Cryptol. Conf. Adv. Cryptol., vol. 3152, pp. 41–55.

[10] E. Bresson, J. Stern, and M. Szydlo, 2002 , "Threshold ring signatures and applications to ad-hoc groups," in Proc. 22nd Annu. Int. Cryptol.Conf.Adv. Cryptol., vol. 2442, pp. 465–480.

[11] J. Camenisch, 1997 , "Efficient and generalized group signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., vol. 1233,pp. 465–479.

[12] N. Chandran, J. Groth, and A. Sahai, 2007 , "Ring signatures of sub linear size without random oracles," in Proc. 34th Int. Colloq. Automata, Lang. Programming, vol. 4596, pp. 423–434.

[13] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, 2012 , "Social cloud computing: A vision for socially motivated resource sharing," IEEE Trans.Serv.Comput.,vol.5,no.4,pp.551 563,FourthQuarter.

[14] D. Chaum and E. van Heyst, 1991 , "Group signatures," in Proc. Workshop Theory Appl. Cryptographic Techn., vol. 547, pp. 257–265.

[15] L. Chen, C. Kudla, and K. G. Paterson, 2004 , "Concurrent signatures," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., vol. 3027, pp. 287–305.

[16] H.-Y. Chien, 2008 , "Highly efficient ID-based ring signature from pairings," in Proc. IEEE Asia-Pacific Serv. Comput. Conf.,pp. 829–834.

[17] S. S. Chow, R. W. Lui, L. C. Hui, and S. Yiu, 2005, "Identity based ring signature: Why, how and what next," in Proc. 2nd Eur. Public Key Infrastructure Workshop, vol. 3545, pp. 144–161.

[18] S. S. M. Chow, V.K.-W. Wei, J. K. Liu, and T. H. Yuen, 2006 , "Ring signatures without random oracles," in Proc. ACM Symp. Inform., Comput., Commun. Security , pp. 297–302.

[19] S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui, 2005 , "Efficient identity based ring signature," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, 2005, vol. 3531, pp. 499–512.

[20] R. Cramer and V. Shoup, 1999 , "Signature schemes based on the strong RSA assumption," in Proc. ACM Conf. Comput. Commun. Security , pp. 46–51.

[21] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, 2004 , "Anonymous identification in Ad Hoc groups," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., vol. 3027, pp. 609–626.

[22] L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen , 2009, Practical short signature batch verification," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., vol. 5473, pp. 309– 324 .

[23] J. Han, Q. Xu, and G. Chen , 2008 , "Efficient ID-based threshold ring signature scheme," in Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Computing., pp. 437–442.

[24] J. Herranz, 2007, "Identity-based ring signatures from RSA," Theor. Comput. Sci., vol. 389, no. 1-2, pp. 100–117.

[25] J. Herranz and G. S_aez , 2003 , "Forking lemmas for ring signature schemes," in Proc. 4th Int. Conf. Cryptol. India, vol. 2904, pp. 266–279.

[26] M. Klonowski, L. Krzywiecki, M. Kutylowski, and A. Lauks, 2008 , "Step-out ring signatures," in Proc. 33rd Int. Symp. Math. Found. Comput. Sci., vol. 5162, pp. 431–442.

[27] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, 2013, "Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143.

[28] D. Y. W. Liu, J. K. Liu, Y. Mu, W. Susilo, and D. S. Wong, 2007 , "Revocable ring signature," J. Comput. Sci. Tech., vol. 22, no. 6, pp. 785–794.