Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud

K.Govinda,
School of Computing Science & Engg,
VIT University,Vellore-14,India.

Dr.E.Sathiyamoorthy,
School of Information Technolory & Engg,
VIT University,Vellore-14,India.

Abstract— **Cloud computing is the best solution for providing a flexible, on-demand, and dynamically scalable computing infrastructure for many applications. In case of private cloud environment access is limited to a group of users or an organization. Even though there are many aspects in cloud environment. The data security, confidentiality and privacy plays a major role in cloud deployment model. In private cloud the identity anonymization and secured data storage becomes essential to address. In this paper a method for identity anonymization and secure data storage in private cloud using GDS (Group Digital Signature) is proposed and implemented.**

Keywords- Group Signature, Identity, RSA, Group Manager, Members.

I. INTRODUCTION

All standard paper components have been specified for three reasons: In cloud computing infrastructure Digital identity management is one of the challenging task. In order to provide access control in a flexible manner to the users based on their identity and past interaction histories the user is authenticated .At the same time confidentiality of the user must be maintained and interoperability across the multiple business domains can be achieved and minimizing the method of Identity verification. In a group digital signature scheme the users of the group can sign behalf of the group. The signatures are basically anonymous, which leads to the Identity anonymization of the real signer(user) in the group with an exception for the group manager. The signatures are verified by using single group key. Group Signature is valid only when it offers anonymity of the signer to others and traceability to the group manager. This feature of the Group digital signature made it as the part of many security applications[1].J. Camenisch and M. Stadler who published the first Group digital signature scheme with constant sized group public key and group signature as a asymmetric crypto system[2]. The theoretical foundations from M.Bellare, D.Miccianicoand B.Warinschigroup digital signature developed it self with the group scheme variant from chang in which he let the user of the group to sign the message to form a partial signature and the procedure combine to form a signature for the user by the group as in the method of threshold crypto system. Later Shamir lifted the method of digital signature through his concept of ID based crypto system which is based on the certificate that lead to the simplification of key management procuders in Public Key Infrastructure (PKI).As a turning point S. Park, S. Kim and D. Won join hands and combined stalder's e th root verification encryption and shoemakers method and proposed first Id based Group digital signature scheme. Like wise being an entry level technique, here we used the concept of key sharing with DH algorithm and strong RSA algorithm to generate keys and for signing in a simple and secured manner. We also include the technique of encryption for data security and signature for authentication.

II. LITERATURE REVIEW

A. *Private Cloud*

The cloud computing environment which incorporates confidential network computing is said to be the Private cloud or internal cloud. This computing environment developed for the exclusive use of single organization or user, providing complete control over data, security and QOS. It is a deployment module which is mostly used for large corporations with recourses located in multiple locations for providing cloud services over the corporate network to its internal users in a highly secured manner as shown in Figure1. The advancement in virtualization, multi-tenancy and data center consolidation makes community network and data center administrators to provide cloud services efficiently to meet the requirements of the customer's within the corporate. Cloud environment allows large organizations from "resource pooling" concept connected with the cloud and its size. Apart from this the issues like data Security, Corporate governance are needs to be considered

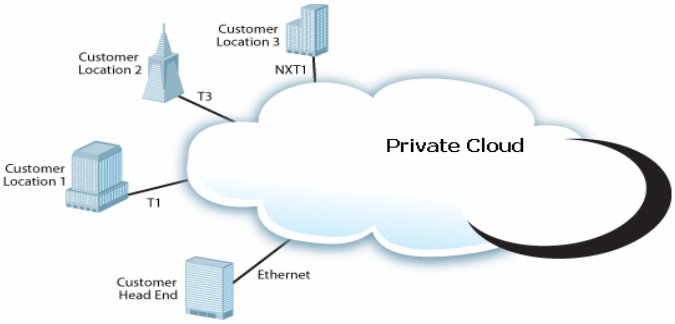


Fig1. Private Cloud accessed in multiple locations

B. Group Digital Signature

The Group Signature methodology can be defined as the signing scheme proposed for groups which benefits by giving authority to the member in the team or group to sign instead of his team. Consider a faculty belongs to a university is sending a message to cloud there for the cloud provider it is enough to know that some authorized person in the university had signed the message this convenience can be provided by this signature scheme[2]. In Group signature method the group manager forms the foundation not only because he manages the team but also for the reason that he is the one who can reveal the identity of the anonymized signer which is one of the great deals in this scheme of signing. The group signature variant is accepted only when it provides anonymity[6-7], unforgeablity, traceability and non-likability.

C. Key Distribution with Diffie-Hellman

DH (Diffie-Hellman) is a key distribution algorithm that helps two users to share secret key between them without the need to exchange the secret key[5]. An overview of the algorithm is given below in Fig2.

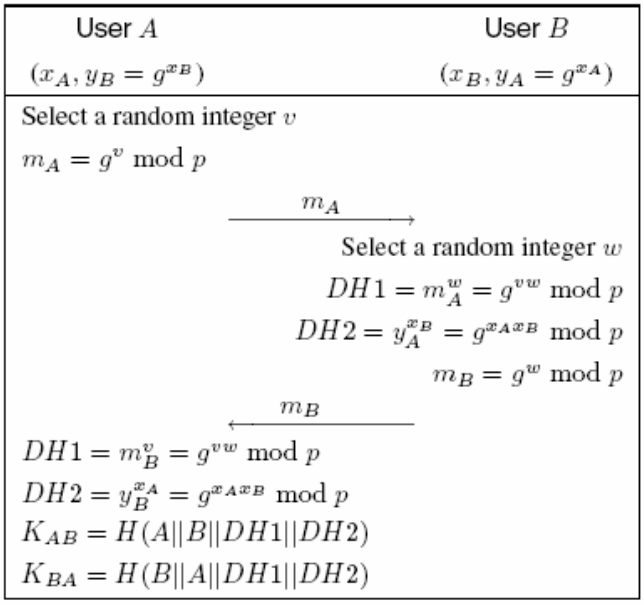


Fig2. Diffie- Hellman key exchange scheme

D. Data Encryption, Decryption and Signature with RSA

RSA is a public key algorithm developed by Rivest, Adi Shamir and Len Adleman that is used for Encryption, Decryption, Signature and Key Agreement. RSA algorithm uniquely uses keys of size 1024 to 2048. Overviews of RSA algorithms are given below.

RSA Key generation

- Select two large prime numbers p and q.
- Compute n=p*q. The computed n is made public.
- Now compute Φ(n) = (p-1) (q-1)
- Choose a random number 'α' as the public key in the range 0< α < Φ(n) such that
  gcd (α, Φ (n)) = 1.
- Find private key d such that $\beta = \alpha^{-1}$ modulus Φ (n).

Encryption

- Consider the user A that needs to send a message to B in a secured manner using RSA algorithm.
- Now α is B's public key. Since α is public, A is allowed access to α.
- For encryption the message M of A which is in the range 0<M<n is converted to cipher.
- Where the Cipher text $C = M^{\alpha}$ modulus n.

Decryption

- Now the cipher text C is sent to B from A.
- User B calculates the Message with its private key β, where message $M = C^{\beta}$ modulus n.

III. PROPOSED METHOD

Here we used the strong RSA Algorithm for the generation of keys as well as for the process of encryption, decryption and signature. In the proposed method the protocol can be given as

The group manager shares a secret key between himself and the cloud provider. This key is considered as the secret group id. In the group the group manager receives the user id (member identity) from the member and the gives the key pair (α, β_i).

- α – Public Key (Common all over the group)
- β_i - Private Key (Unique key given to the member as per the value of i)

The member now can sign any message with the provided β_i. The message is encrypted or signed as the procedure explained below and send to the group manager. The group manager authenticates the member and then collects the details required and attaches the secret group id and signs it and sends it to the cloud provider. The cloud provider authenticates the message and allows the encrypted message to be stored inside the private cloud.

A. Group Secret key Sharing

In this proposed method the secret group key is the key distributed between the group manager and the cloud provider using the Diffie-Hellman's algorithm of key distribution.

B. Group manager's phase

The group manager selects the public key α based on some specified condition. Then the group manager generates different values p_i and q_i with respect to the strong RSA algorithm in order to generate β_i. Where $\beta_i = \alpha^{-1}$ modulus $(\Phi n)_i$, and $((\Phi n)_i = p_i\text{-}1 * q_i - 1)$. According to the strong RSA algorithm the public key α is selected in such a way that it satisfies the following conditions.

- GCD of (α , n) = 1, and
- The public key α is always 0 < α < n. (n = p * q)

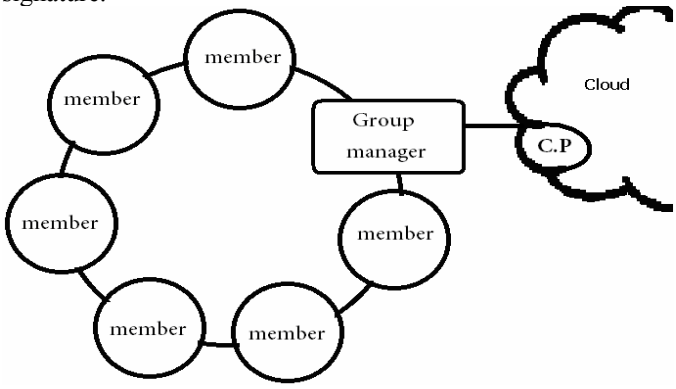
Hence while using this method α must be a prime number and can be comparatively small. Since α is prime number irrespective to the n, GCD of (α,n) = 1. On comparison n will be surely greater than α.

TABLE I. TABLE MAINTAINED BY THE GROUP MANAGER FOR KEY DISTRIBUTION (A=7 IS COMMON)

Member id	P	Q	n=p*q	Φn= p-1*q-1	Private key β
10001	11	13	143	120	496325
10004	7	17	119	96	558634
10005	11	7	77	60	443673
10003	7	13	91	72	435672
10002	17	11	187	160	512351

C. Member's phase

At first the member connects with the group manager and gives his id. The group manager receives the id and issues a private key β_i. The private key β_i is now used for signature.



D. Procedure for storing the data

The data is encrypted with the public key α. Then an attachment that consists of signed member id and message digest is sent to the group manager the manager verifies the signature with the signature with the group's public key α and then removes the attachment. The group manager again makes an attachment which consists of the signed secret group id and the encrypted member's data. The set is now sent to the cloud provider.

E. Cloud provider's phase

The cloud provider decrypts the signature with the group's public key α to find out the genuine group members and stores the data in the cloud.

CONCLUSION

In this paper we proposed a protocol in which the group digital signature is generated using the strong RSA algorithm. In this method the freedom of the member is sacrificed by sending the message through the group manager. In future this protocol will be re modified with member's freedom to send the data directly in the cloud but at the same time we have to keep in mind that traceability of user by the group manager must be maintained.

REFERENCES

[1] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital. Signatures and Public-Key Cryptosystems," The Technical Paper to Laboratory for Computer Science,Massachuset Institute of Tech,Cambridge.

[2] Yong Hao, Yu Cheng, and Kui Ren , Distributed Key Management with Protection against RSU Compromise in Group Signature based VANETs, 3rd ed., vol. 2. IEEE BLOBECOM 2008.

[3] Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem," RSA Laboratories

[4] P. Kitsos, N. Sklavos and O. Koufopavlou, "An efficient implementation of the digital signature algorithm," IEEE 2008.

[5] Diffe, W., and Hellman, M." New directions in cryptography. IEEE Trans. Inform. Theory IT-22", (Nov. 1976), 644-654.

[6] G.. M. Liu, Very simple schemes for group signatures, master thesis, Chung Yuan Christian University, June 2003.

[7] D. Chaum and E. van Heyst, "Group signatures," *In Andances in Cryptology – EUROCRYPT'91*, vol. 547, pp. 257-265, 1991.

AUTHORS PROFILE

Prof .K.Govinda working as an Assistant Professor in School of Computing Science and Engineering of VIT University, Vellore, Tamil Nadu. He has more than X years of teaching experience and his areas of interests are Database, Distributed Database, Data Warehousing , Data Mining and Cloud Computing.

Dr.E.Sathiyamoorthy working as an Associate Professor in School of Information Technology and Engineering of VIT University, Vellore, Tamil Nadu. He has more than XII years of teaching experience and his areas of interests are Web Services, E-Commerce and SOA.