A New Framework for Group Signature Based Upon PAVD Security System

Rakesh Kumar
Department of Computer Science & Engineering
Guru Nanak Dev University
Amritsar, 143001, India

Abstract: **This paper has focus on group based PAVD security system. The three security issues of Privacy, Authentication, and verification of data. The PAVD system use of two different servers' via. (1) Encryption server (2) storage server. The group signature procedure can be define as the signing scheme planned for groups which benefits by giving power of the member in the team or group to sign instead of his team. In the group signature process the group manger forms the foundation not only because he managers the teams but also for the reason that he is the one who can reveal the identity of anonymized signer. In this paper a method for identity anonymization and secure data with PAVD security system with respect to uploading and downloading time using GDS (Group Digital Signature) is proposed and implemented.**

Keywords: PAVD, Cloud Computing, Stakeholders, Security Problem, Data Secrecy, SHA, Group Based Signature, CSP, AES .

I. INTRODUCTION

Cloud Computing, being in their infancy in the field of research has attracted a lot of investigation societies in last few years. Lot of investment is created in cloud based research by MNCs like Amazon, IBM organizations. Inspite of those the number of stakeholders really using cloud services is limited. Cloud computing is a pool of configurable causes and services. User is simply expected to generate an consideration with the cloud service provider like Amazon, Google, Rackspace, CloudBees, dotcloud, Savvis and so on to get into different cloud services. Cloud service vendors provide number of companies including Mint, CloudMe, Cloudo, Drop box and several more (Nisha Lodha et al. 2014)[1].

The concept of group signatures was first proposed by (D. Chaum et al. 1991). The most recent scheme by (Ateniese et al. 2000) is particularly effective and provably protected. Unfortunately a few limitations however provide all past answers poor in practice. One essential problem is how to deal with coverage of group signing recommendations.

The Concept of a Group Signature Structure consists of the four procedures like setup, sign, verify, and open [2].

Group signature [3] schemes are an essential building block for many security applications. On the other hand to ordinary signature schemes where there's only 1 signer, group signature schemes allow any member of a group of signers to sign documents on behalf of the group. Generally, a group manager controls the group membership and issues group signing secrets to group members. The group signing secrets allow a group member to sign documents on behalf of the group. Specifically, a group signature system gives secrecy and unlinks ability to the signer, i.e. every one may examine that the signature is legitimate on behalf of a group, but no one with the exception of the group manager may identify the signing member.

In this report we mentioned The Three-In-One Security mechanism addresses three security issues of privacy, data security and data verification. Hence it is called as PAVD [4] system. PAVD stands Privacy, Authentication and Verification of data. Hence PAVD program we're utilizing two various servers' viz. Encryption server and Storage server. The encryption server perform three responsibilities: Firstly key exchange using Diffie Hellman Key trade algorithm with the customer, Secondly assess SHA-1 code for the original file for verifying digital signature at the time of downloading and lastly encryption user data using RSA encryption algorithm.

In this paper we proposed a PAVD security system by using group based signature. In section 2 related works concerning group signature is discussed. section 3 more formally describe the various gaps and in section 4 algorithms are proposed that solve the gap. Finally section 5 concludes this paper.

II. RELATED WORK

(G. Jai Arul Jose et al. 2011) propose to produce RSA public key and Private Key for public and private access to overcome the situation of data security .Binary record can be used inside get a control on node setup record to create sure cloud data flow securely. The get a control on node deliver data through protected Socket Layer after activation. Ultimately AES algorithm is use for encryption .this unique mixture makes this answer best to prevent different types of attacks. The strength of their function is solid data security against different assault. if consumers is attempt to login wrongly for often, the device automatically slowing the services and temporarily end the account services for this consumer [5] .

(Girault et al. 1998) [6] investigates notion just like in which of key insulation associated with a digital signatures while context of cards research. Nonetheless, this particular initial function doesn't have any formal unit with no proofs associated with security. Efforts on key-insulated public-key encryption were thought to be simply by (Dodis, Yevgeniy) [7] and also (Lu et al. 2002) [8] (but simply next to a weak non-adaptive adversary). Key-insulated public-key encryption was first formalized, as well as strategies with extensive proofs of security given, inside the current function associated with (Dodis et al. 2002) [9].

According to (Kanika et al. 2010) [4] In Cloud computing, we have issue like security of data, documents process, backups, Network traffic, host security .They have proposed a idea of digital signature with RSA algorithm, to encrypt the data while moving it within the network. This approach solves the dual issue of authorization and security. The strength of their work is the structure proposed to address security and privacy issue.

(Hatem S. Abdelkader et al. 2012) [10] Cloud computing moves the application software and listings to the large data centers, where the administration of the data and solutions may not be fully trustworthy. This excellent feature, but, increases many new security challenges. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. Therefore their report investigates the essential issue of cloud computing data security. They presented the data security model of cloud computing on the basis of the study of the cloud architecture. They executed software to improve perform in a data security model for cloud computing. Eventually they used that software in the Amazon EC2 Micro example for evaluation process.

(Ayush Sharma et al. 2012) claims a fresh method called cloud networking which gives networking functionalities to cloud computing and helps flexible placement of virtual assets crossing provider borders. This enables several types of optimization, e.g., lowering latency or network load. This report presents a security architecture that allows an individual of cloud networking to define security requirements and enforce them in the cloud networking infrastructure [11].

As per (Deyan Chen et al. 2012)from the consumers perception, cloud computing security concerns are specially data security and privacy defense problems which remain the primary inhibitor for use of cloud computing services. They provided a concise but all-round analysis on data security and privacy defense problems related with cloud computing across all phases of data life cycle. Chances are they proposed to protect data using different scheme and procedures like airavat etc. This method can reduce privacy loss without authorization in Map-Reduce computing process. The weakness is that it just a concept which depends on other scheme and procedures because of its implementation [12].

(K. S. Suresh et al. 2012) This paper discusses about the basic cloud features like Iaas , Paas and SaaS and also provided information that if data is kept at any cloud sever , then it can be kept in encrypted form so that when someone even tries to access the data base , then hacker should not get the data directly . For the encryption mechanism three good encryption algorithms namely AES , MD5 and RSA are discussed. The problem with this approach is that, this paper doesn’t taking about any combinational algorithm for encryption which is quite feasible these days [13].

(Dr.A.Padmapriyaet al. 2013) This paper have discussed about cloud computing security mechanisms and presented the comparative study of several algorithms .After discussing the general problems of the cloud computing server application , introduces a heterogeneous mode algorithm which is a combination of two or more security algorithms. This paper talks about the RSA and DES algorithm and provides information that they can be combined to create a new algorithm for the encryption part [14].

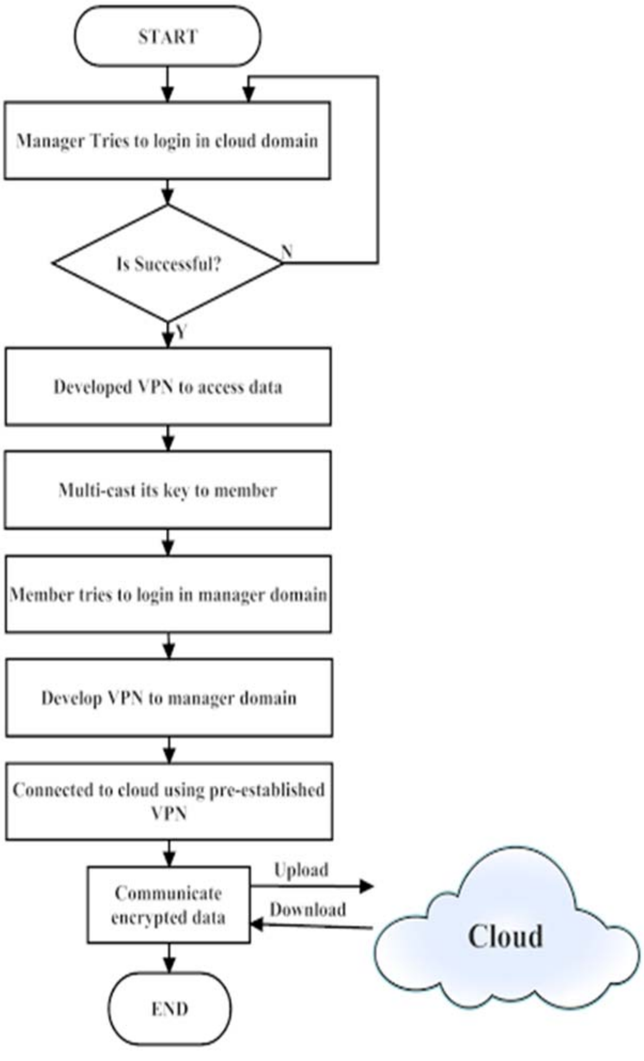
(Priyanka Gupta et al. 2013) This paper explores a new method which is a combination of role based access control with advanced encryption algorithm (a combination of RSA and two fish),signature verification to enhance security when storing text, image ,audio ,video files onto cloud server [15].

III. GAPS IN LITERTURE

By conducting the review it has been found that most of the existing literature.

- The use of group based signature in PAVD security system has been ignored.
- The majority of secured data storage has neglected. The login overhead has been neglected.
- The member freedoms to upload and download data have algorithms ignored in existing research.

IV. METHODOLOGY PROPOSAL


START
Manager Tries to login in cloud domain
Is Successful?
N
Y
Developed VPN to access data
Multi-cast its key to member
Member tries to login in manager domain
Develop VPN to manager domain
Connected to cloud using pre-established VPN
Communicate encrypted data
Upload
Download
Cloud
END

Following are the steps required to successfully simulate the proposed system:

Step 1: Initialize GM Manager Try to Login in Cloud Domain.

Step 2: Is successful then developed VPN to Access data.

Step 3: GM Shared SK with CSP. SK also acts as group id. Then the GM generates different values pi and qi with respect to the strong AES algorithm in order to generate di. Where di = (e - 1) mod f(n), Where f(n) = pi *qi - 1.

Step 4: The GM receive U id MI & share KP e, di. Here e PKC di PKU.

Step 5: The M (member) initiate the login Process.

Step 6: Develop VPN to Manager Domain.

Step 7: Connected to cloud using Pre-established VPN.

Step 8: Apply encryption algorithm A. algorithm A encrypt the message and

send to the GM.

Step 9: GM authenticates the member and then gathers the information essential and assigns, the secret G id and sends it to CP.

Step 10: Now can Communication Data (upload and download) by using Manager accesses. Algorithm For

(A) Upload Section:

1. The information is encrypted with the PK e.
2. Then an attachment that involve of signed M id. And message summary is send to the GM. The M conforms the sign with G PK e and then removes the attachment.
   The GM again makes attachments which consists of the sign SG id and then encrypt MD.
3. Look the data to be uploaded.
4. Member encrypts the data with his key and mentions it to the server.
5. Then the encrypted server decrypts the data with his key.
6. Calculate the group based signature using SHA-1 algorithm for original data and store it for the verification purpose at the time of downloading.
7. Finally the encryption server encrypts the data with its key using AES.
8. Now Member accesses the storage server through the manager domain and uploads the data to the cloud.

(B) Algorithm for File Downloading

1. Choice the data to the download from Fetch data list.
2. User demand for the data from Storage server by clicking on download button.
3. The data is then sent to the encryption server by the customer.
4. Then encryption server decrypts the data with its key.
5. It computes the group based signature using SHA-1 algorithm for the decryption data and match.
6. If the later signature is found to match with the database entry then data is verified if the data is correctly verified then data is downloaded.

Step 11: GSK sharing GSK is the key distributed between the GM and the CP using Diffe-Hellmans algorithms.

Pseudo Code for implantation of the Diffe-Hellman Key Exchange Algorithms Sender Receiver

Step: 1 Input the DH factors a, b and a smallest value for the Public Key SR.

Step: 2 Create Public Key SR and a Private key SR using the integer and AES technique.

Step: 3 Use the Sender Receiver code module to first send Public Key SR as a integer to the Receiver Sender and then receive Public Key RS as a integer and Receiver Sender.

Step: 4 Generate the DH factors c as a big integer and calculate ac mod b as a big integer.

Step: 5 Encrypt ac mod b using Public Key RS and generate the cipher big internet: E (public Key RS, ac mod b).

Step: 6 Use the Sender Receiver code component to first send E(public Key RS, ac mod b) as a big integer to the Receiver Sender and then receiver E(public Key SR, ac mod b)as a big integer from Receiver Sender.

Step: 7 Decrypt E (public Key SR, ad mod b) using Private Key SR and extract ad mod b as a big integer

Step: 8 Compute (ad mod b) c mod b as a big integer and this is a secrete session key granted by both sides.

After the success full connection establishment, key exchange, encryption, decryption the data transfer tool place, after which the connection is terminated.

GM Phase: The GM selects the PK based on some specified conditions. Then the GM generates different values with the help of strong algorithm.

M phase: At the firstly M links with the GM and provides his id. The GM accepts the id and issue a private key di. The P (private) key di is now used for signature.

CSP phase

Step 1: CP decrypts the signature with the group PK e.

Step 2: store the data in C.

Table: Description of the notions that used in this paper

Notation	***Description***
GM	Group Manager
M	Member
PK	Public key
SK	Secret Key
CSP	Cloud Service Provider
PKC	public key Common all over the group
KP	Key Pair
PKU	public key Unique given to the member as per the value of i
MI	Member Identity
U	User
E	Public Key
d_i	Private Key as per value of i.
GSK	Group secret key

V. CONCLUSION

This paper has offered a new framework which is based on group based signature to reduce communication overheads in PAVD security system. The group based signature will enhance the data storage and also provide the freedom to group member to send and receive data directly which will reduce the authentication overheads. To evaluate the upload and download time like amazon cloud drive, box, drop box etc. To draw comparison between PAVD security system and proposed group based digital signature based upon the following parameters: Download and Upload time, Overheads , End to End delay ,Response Time, Execution Time and energy. The overall objective of this paper is to offer a PAVD security system which is based upon Group based signature to reduce login overheads and evaluate the upload and download time .

In near future we will design and implements proposed technique in MATLAB Tool with the help of MATLAB Tool Box also to use some quality measure to evaluate the effectiveness of the proposed technique.

REFERENCE

[1] Yogita Pawar, Prashant Rewagad, Nisha Lodha "Comparative Analysis of PAVD Security System with Security Mechanism of Different Cloud Storage Services" 2014 Fourth Internationa,l Conference on Communication Systems and Network Technologies, 2014 IEEE.

[2] Ateniese, Giuseppe, Jan Camenisch, Marc Joye, and Gene Tsudik. "A practical and provably secure coalition-resistant group signature scheme." InAdvances in Cryptology—CRYPTO 2000, pp. 255-270. Springer Berlin Heidelberg, 2000.

[3] K.Govindaa,Dr.E.Sathiyamoorthyb "Identity Anonymization and Secure Data Storage usingGroup Signature in Private Cloud" 2212-0173, 2012 Published by Elsevier Ltd.

[4] Uma Somani, Kanika Lakhani, Manish Mundra " Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing "2010 IEEE Ist International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).

[5] G. jai Arul Jose, c. sajeev, Dr. C. Suyambulingom " Implementation of Data Security in Cloud computing" International Journal of P2P Network Trends and Technology –Volume Issue1-2011.

[6] Girault, Marc. "Relaxing tamper-resistance requirements for smart cards by using (auto-) proxy signatures." In Smart Card Research and Applications, pp. 157-166. Springer Berlin Heidelberg, 2000.

[7] Dodis, Yevgeniy, Jonathan Katz, Shouhuai Xu, and Moti Yung. "Key-insulated public key cryptosystems." In Advances in Cryptology—EUROCRYPT 2002, pp. 65-82. Springer Berlin Heidelberg, 2002.

[8] Cheng-Fen, Lu, and ShiuhPyng Winston Shieh. "Secure key-evolving protocols for discrete logarithm schemes." In Topics in Cryptology—CT-RSA 2002, pp. 300-309. Springer Berlin Heidelberg, 2002.

[9] Dodis, Yevgeniy, Jonathan Katz, Shouhuai Xu, and Moti Yung. "Strong key-insulated signature schemes." In Public Key Cryptography—PKC 2003, pp. 130-144. Springer Berlin Heidelberg, 2002.

[10] Sherif el-etriby, Eman m. Mohamed and hatem s. Abdelkader Published "Modern Encryption Technology for cloud computing Randomness and Performance Testing" in the third International Conference on Communications and Information Technology ICCIT 2012.

[11] Volker Fusening and Ayush Sharma "Security Architecture For Cloud Networking "2012 IEEE International Conference on Computing, Communication and Network, Cloud Computing and Networking Symposium.

[12] Deyan Chen and Hong Zhao " Data Security and Privacy Protection Issue in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[13] K. Suresh and K. Prasad, Security issues and security algorithms in cloud computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 10, 2012.

[14] Padmapriya, Dr A., and P. Subhasri. "Cloud Computing: Security Challenges & Encryption Practices." International Journal of Advanced Research in Computer Science and Software Engineering 3, no. 3 (2013): 255-259.

[15] Mr.Prashant Rewagad and Ms. Yogita Pawar. " Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorthims to Enhance Data Security in Cloud Computing" 2013 IEEE International Conference on Communication system and Network Technology.