SeCt-Cloud – Security Certificate Based Reliable and Confidential Data Storage in Cloud

S.BALAVINOTH,PG Scholar,
Department of Computer Science & Engineering, ,
J.K.K.Munirajah College of Technology,Tamilnadu
balavinoth2008@gmail.com

N.SATHYA BALAJI M.E.,Professor
Department of Computer Science & Engineering
J.K.K.Munirajah College of Technology,Tamilnadu
sathyabalajin@gmail.com

ABSTRACT:

Secure data storage in cloud having more problems like insider threats as legitimate and malicious users from outsiders. In this project, propose SeCt-Cloud – Security Certificate based data storage in cloud. The SeCt-Cloud methodology uses the group certificate for data sharing in cloud. Each group has an individual signature certificate for secure data sharing within the group. The certificate less malicious users can't able to access the file. Also the insider threats can't access the file without the updated certificate.This (SeCt-Cloud) methodology that provides: Certificate Generation, Certificate Access Control List Maintenance,Certicate Verification, Data confidentiality,integrity,Access control, Data sharing,Insider threat security, Forward and backward access control.The SeCt-Cloud methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeCt-Cloud methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. In this model, a certificate – or, more generally, a signature – acts not only as a certificate but also as a decryption key. To decrypt a message, a key holder needs both its secret key and an up-to-date certificate from its CA Certificate-based encryption combines the best aspects of identity-based encryption and public key encryption.

1.INTRODUCTION

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers. Organizations with a low budget can now utilize high computing and storage services without heavily investing in infrastructure and maintenance. The loss of control over data and the storage platform also motivates cloud customers to maintain the access control over data (individual data and the data shared among a group of users through the public cloud). Moreover privacy,confidentiality of the data is also recommended to be cared for by the customers.The confidentiality management by a customer ensures that the cloud does not learn any information about the customer data. Cryptography is used as a typical tool to provide

IJIREST

confidentiality and privacy services to the data.

2.RELATED WORK

2.1 GENERAL:

Cloud computing has been envisioned as the next generation information technology architecture for enterprises, due to its long list of unprecedented advantages in the IT history:on-demand self-service,location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications.cloud computing is transforming the very nature of how businesses use information technology.From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits:relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software,maintenances, etc.

2.2 CLOUD COMPUTING

In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time.The phrase is also more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines.

ADVANTAGES

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. This can work for allocating resources to users. For example, a cloud computer facility, which serves European users during European business hours with a specific application (e.g. email) while the same resources are getting reallocated and serve North American users during North America's business hours with another application (e.g. web server).

2.3 SERVICES IN CLOUD:

Cloud computing is mostly used to sell hosted services in the sense of application service provisioning that run client server software at a remote location. Such services are given popular acronyms like 'SaaS','PaaS' ,'IaaS', 'HaaS' and finally 'EaaS'.End users access cloud-based applications through a web browser, thin client or mobile app while the business software and user's data are stored on servers at a remote location.

3. RECENT METHODOLOGY

In previous work CL-PRE, a certificate less proxy re-encryption scheme for secure data sharing with public cloud. In CLPRE, a data owner encrypts shared data in cloud with an encryption

IJIREST

key, which is further encrypted and transformed by cloud, and then distributed to legitimate recipients in accordance with access control.

Uniquely, the cloud-based transformation leverages re-encryption keys derived from private key of data owner and public keys of receipts, and eliminates the key escrow problem in identity based cryptography and the need of certificate.While preserving data and key privacy from semi-trusted cloud, CL-PRE leverages maximal cloud resources to reduce the computing and communication cost for data owner. Towards running proxy in public cloud environment, further use multi-proxy CL-PRE and randomized CL-PRE, which enhance the security and robustness of CL-PRE. To implement all CL-PRE schemes and evaluate their security and performance.A certificateless proxy re-encryption (CL-PRE) scheme for securely sharing the data within a group in the public cloud.

In the CL-PRE scheme, the data owner encrypts the data with the symmetric key. Subsequently, the symmetric key is encrypted with the public key of the data owner. Both the encrypted data and the key are uploaded to the cloud.The encrypted key is re-encrypted by the cloud that becomes decrypt able by the user’s private key.

DISADVANTAGES

The computational cost of the bilinear pairing is high as compared with the standard operations in finite fields.This methodology based on the shared key derivation method for securing data sharing among a group. The methodology uses a binary tree for the computation of keys. However, the computational cost of the proposed scheme is high as the rekeying mechanism is heavily employed.

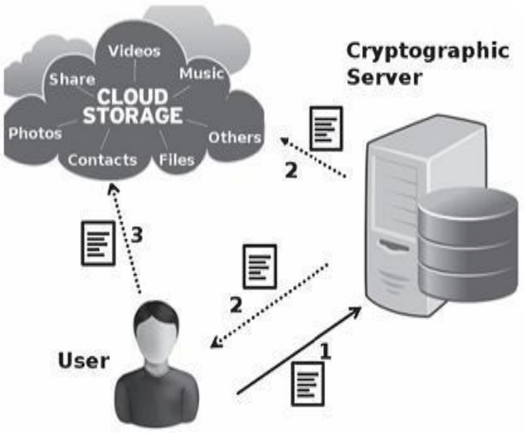
4. PROPOSED SYSTEM

In this project, propose a methodology named security certificate based data storage that deals with the aforementioned security requirements of shared group data within the cloud. The proposed methodology ensures the confidentiality of the data on the cloud by using symmetric encryption. The secure data sharing over the cloud among the group of users is ensured without the elliptic curve or bilinear Diffie–Hellman problem (BDH) cryptographic re-encryption. The possession of a portion of the key secures the data against malicious insiders within the group. The proposed SeDaSC methodology secures the data against issues of forward and backward access control that arise due to insider threats.To perform formal modeling and verification of the SeDaSC methodology by using high-level Petri nets (HLPNs), the Satisfiability Modulo Theory Library (SMTLib), and a Z3 solver.The SeDaSC methodology works with three entities as follows:1) users; 2) a cryptographic server (CS); and 3) the cloud.The data owner submits the data, the list of the users, and the parameters required for generating an access control list (ACL) to the CS. The CS is a trusted third party and is responsible for key management, encryption, decryption, and access control. The CS generates the symmetric key and encrypts the data with the generated key. Subsequently, for each user in the group, the CS divides the key into two parts such that a single part alone cannot regenerate the key. Successively, the original key is deleted through secure overwriting. One part of the key is transmitted

IJIREST

to the corresponding user in the group, whereas the other part is maintained by the CS within the ACL related to the data file. The ACL is generated through the parameter submitted by the data owner.

The encrypted data are subsequently uploaded to the cloud for storage on behalf of the user. The user who wishes to access the data sends a download request to the CS. The CS, after authenticating the requesting user, receives the portion of the key from the user and subsequently downloads the data file from the cloud. The key is regenerated by operating on the user portion of the key, and the corresponding CS maintained portion for that particular user. The data are decrypted and sent back to the user. For a newly joining member, the two portions of the key are generated, and the user is added to the ACL. For a departing member, the record is deleted from the ACL.



The departing member cannot decrypt the data on its own as he/she only possesses a portion of the key. Similarly, no frequent decryption and re-encryption are needed in case of changes in the group membership. Moreover, SeDaSC can be used with the mobile cloud computing paradigm in addition to conventional cloud computing due to the fact that compute-intensive operations are performed by the CS.

5. MODULES AND DESCRIPTION

5.1 CERTIFICATE GENERATION

Certificate is generated for each user and data owner during their registration. A (digital) certificate is a signature by a trusted certificate authority (CA) that securely binds together several quantities. Typically, these quantities include at least the name of a user U and its public key PK. Often, the CA includes a serial number SN (to simplify its management of the certificates), as well as the certificate's issue date D1 and expiration date D2. By issuing SigCA(U, PK, SN, D1, D2), the CA basically attests to its belief that PK is (and will be) user U's authentic public key from the current date D1 to the future date D2. Since CAs cannot tell the future, circumstances may require a certificate to be revoked before its intended expiration date.For example, if a user accidentally reveals its secret key or an attacker actively compromises it, the user itself may request revocation of its certificate. Alternatively, the user's company may request revocation if the user leaves the company or changes

IJIREST

IJIREST

position and is no longer entitled to use the key. If a certificate is revocable, then third parties cannot rely on that certificate unless the CA distributes certificate status information indicating whether the certificate is currently valid.

5.2 MAINTAINING CERTIFICATE REVOCATION LIST

Certificate revocation list (CRL) is simply a list of certificates that have been revoked before their intended expiration date. The CA issues this list periodically, together with its signature. Since the CA will likely revoke many of its certificates – say, 10% if they are issued with an intended validity period of one year – the CRL will be quite long if the CA has many clients. Nonetheless, the complete list must be transmitted to any party that wants to perform a certificate status check. There are refinements to this approach, such as delta CRLs that list only those certificates that have been revoked since the CA's last update.

5.3 FILE ENCRYPTION AND UP LOADING :

Each file which is to be uploaded is encrypted with encryption key. Once file is encrypted, next step is to upload it to the storage system along with data decryption key. Owner specifies the set of attributes for access structure, it then encrypts the file. Finally, owner uploads encrypted file and encryption key and set of attributes to the storage system.

5.4 KEY SHARE GENERATION

K is a random secret generated by the CS for each of the data files. The length of *K* in SeDaSC is 256 bits, as is recommended by most of the standards regarding key length for symmetric key algorithms (SKAs). However, the length of the key can be altered according to the requirements of the underlying SKA. *K* is obtained in a two-step process.

In the first step, a random number *R* of length 256 bits is generated such that *R* = *{*0, 1*}*256. In the next step, *R* is passed through a hash function that could be any hash function with a 256-bit output. In this project used secure hash algorithm 256 (SHA-256). The second step completely randomizes the initial user-derived random number *R*.The output of the hash function is termed as *K* and is used in symmetric key encryption [e.g., the Elliptic Curve Cryptography (ECC)] for securing the data.*CS Key Share Ki:* For each of the

users in the group, the CS generates *Ki*, such that *Ki* = *{*0, 1*}*256. *Ki* serves as the CS portion of the key and is used to compute *K* whenever an encryption/decryption request is received by the CS. Moreover, it is ensured by comparison that the distinct *Ki* is generated for every file user. *User Key Share Ki: K*is computed for each of the users in the group as follows: K1i= $K \oplus Ki.$, *Ki* serves as the user portion of the key and is used to compute *K* when needed.

6.ALGORITHM DETAILS

6.1 ALGORITHM (ECC)

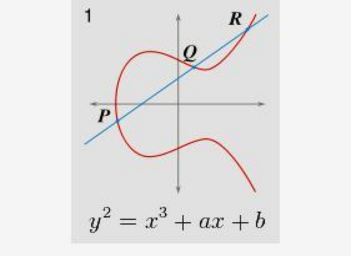
Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington)as an alternative mechanism for implementing public-key cryptography.

$$y^2 = x^3 + ax + b$$

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve n ->Maximum limit



6.2 KEY GENERATION

Key generation is an important part where have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.Now,have to select a number **'d'** within the range of **'n'**.Using the following equation can generate the public key **Q=d*pd** = The random number that have selected within the range of (**1 to n-1**). **P** is the point on the curve.
'Q' is the public key and **'d' is the private key.**

6.3 ENCRYPTION

Let 'm' be the message that are sending. Then have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.Conside *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

DECRYPTION

To get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that have send.

Proof

How does get back the message,

IJIREST

M = C2 – d * C1
‘M’ can be represented as ‘C2 – d * C1′
C2 – d * C1 = (M + k * Q) – d * (k *P)
(C2 = M + k * Q and C1 = k * P)
= M + k * d * P – d * k *P (canceling out k * d * P)
= M (Original Message)

6.3 ECC

Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms have applications cryptography.

Steps:

ECC domain parameters over GF(q), are a sextuple:
T = (q, a, b, G, n, h)

- q = p or q = 2^m
- a and b □ GF(q)

y^2 □ x^3 + ax + b (mod p) for q = p > 3
$y^2 + xy = x^3 + ax^2 + b$ for q = 2^m □ 1

- a base point G = (xG,yG) on E(a,b)(GF(q)),
- a prime n which is the order of G

(The order of a point P on an elliptic curve is the smallest positive integer r such that rP = O.)

- h = #E/n. where #E represents number of points on elliptic curve and is called the curve order.

6.4 ECC KEY GENERATION

A public key Q = (xQ,yQ) associated with a domain parameter (q, a, b, G, n, h) is generated for an entitiy A using the following.
Procedure:

- Select a random or pseudo-random integer d in the interval [1,n-1].
- Compute Q = dG.
- A's public key is Q; A's private key is d.

6.5 ECC KEY VALIDATION

A public key Q = (xQ,yQ) associated with a domain parameter (q, a, b, G, n, h) is validated for an entitiy A using the following
Procedure:

- Check that Q □ O
- Check that xQ and yQ are properly represented elements of GF(q).
- Check that Q lies on the elliptic curve defned by a and b.

IJIREST

- Check that nQ = O.

6.6 ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Proposed by Abdalla, Bellare and Rogaway in 1999.Entity A has domain parameters D = (q, a, b, G, n, h) and public key QA and private key dA. And entity B has authentic copies of D and QA.To sign a message m, A does the following:

Select a random integer k from [1,n-1].Compute kG = (x1,y1) and r = x1

- mod n. If r = 0 then go to step 1.
- Compute k^{-1} mod n. Compute e = SHA-1(m).
- Compute s = k^{-1}\{e + dA . r\} mod n.
- If s = 0 then go to step 1.

A's signature for the message m is (r, s).
To verify A's signature (r, s) on m, B performs the following steps:
Verify that r and s are integers in [1,n-1]

- Compute e = SHA-1(m).
- Compute w = s^{-1} mod n.
- Compute u1 = ew mod n and u2 = rw mod n.
- Compute (x1,y1) = u1G+ u2 QA
- Compute v = x1 mod n.
- Accept the signature if and only if v =r. SHA-1 denotes the 160-bit hash function

6.7 ELLIPTIC AUTHENTICATED ENCRYPTION SCHEME

Analogue of the DSA, proposed by Scott Vanstone in 1992.

- Select a random integer r from [1,n1].
- Compute R = rG.
- Compute K = hrQB = (KX, KY). Check that K □ O:
- Compute k1|| k2 = KDF(KX).
- Compute c = (k1, m). Compute t = MAC(k2, c).
- Send (R; c; t) to B.

ENC a symmetric encryption scheme such as Triple-DES MAC denotes a message authentication code (MAC) algorithm

"RFC 2104" ;

- Perform a partial key validation on R.
- Compute K = hdBR = (KX, KY).. Check that that K □ O:
- Compute k1|| k2 = KDF(KX).
- Verify that t = MAC(k2, c).
- Compute m = ENC^{-1}(k1, c).

IJIREST

7. CONCLUSION

In CL-PRE and SeDaSC, the certificate less encryption is used, this is the way for insider threats and malicious users. Several attacks are mostly occurs without using the certificate. In this project, propose a methodology named Security Certificate based Data storage in Cloud, that deal with the security requirements of shared group data within the cloud. In this new method SeCt-Cloud, Two fish algorithm is used for encryption and decryption of data. The key idea is that certificate-based encryption enables implicit certification without the problems and that implicit.certification allows us to eliminate third-party queries on certificate status, thereby reducing infrastructural requirements and Also described an SeCt cloud scheme that reduces the CA's computation and bandwidth requirements to exceptionally low levels, even though the scheme does not use hash chains or trees like previous PKI proposals.

REFERENCES

1. Revathi Dhamotharan,Eraj Khan,Samee Khan.U "Secure data sharing in clouds" IEEE Systems journal,vol 11 no.2,June 2017

2. Abbas A and S. U. Khan, "A review on the State-of-the-art privacy pre-serving approaches in e-health clouds," *IEEE J. Biomed. Health Informat.*, vol. 18, no. 1, pp. 1431– 1441, Jul. 2014.

3. Alhamazani.K *et al.*, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, state-of-the-art," *Computing*,
DOI: 10.1007/s00607-014-0398-5, 2014, to be published.

4. Chen.D *et al.*, "Fast and scalable multi-way analysis of massive neural data," *IEEE Trans. Comput.*, DOI: 10.1109/TC.2013.2295806, 2014, to be published.

5. Chen.Y and W. Tzeng, "Efficient and provably-secure group key man-
agement scheme using key derivation," in *Proc. IEEE 11th Int. Conf. TrustCom*, 2012, pp. 295–302.

6. Cloud security Alliance, "Security guidelines for critical areas of focus in cloud computing v3.0," 2011.

7. Gutmann.P, "Secure deletion of data from magnetic and solid-state memory," in *Proc. 6th USENIX Security Symp. Focusing Appl. Cryptog-raphy*, 1996, p. 8.

8. Khan.A.N, M. M. Kiah, S. A. Madani,Ali, and S. Shamshir-band,"Incremental proxy re-encryption scheme for mobile cloud computing environment," *J. Supercomput.*, vol. 68, no. 2, pp. 624–651, May 2014

9. Khan A.N, M. L. M. Kiah, S. U.Khan, and S. A. Madani, "Towards secure mobile cloud computing:A survey," *Future Gen. Comput. Syst.*, vol. 29, no. 5, pp. 1278–1299, Jul.13

10. Seo.S, M. Nabeel, X. Ding, and E.Bertino, "An Efficient Certificate-less Encryption for Secure Data Sharing inPublic Clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2107–

IJIREST

2119, Sep. 2013.

11. Wei.L, H. Zhu, Z. Cao, Y. Chen, and V. Vasilakos, “Security and pri-vacy for storage and computation in cloud computing,” *Inf. Sci.*, vol. 258, 371–386, Feb. 2014.

12.Reference https://www.cloud.com/

13.Reference book “cloud security & Privacy” Author Tim Mather.

IJIREST