Securing cloud data by Identity Based Proxy Re-encryption

Mrs. S.Jayashree, Dr. R.S. Sankara Subramanian

Abstract— In a Proxy Re-encryption without seeing the underlying plaintext semi trusted proxy (Cloud Service Provider) converts a cipher text for User A (data owner) into a cipher text for User B (data Storage). In this paper the Identity based proxy re-encryption is used to provide data security while transiting the data from proxy –cloud service provider (CSP) to data storage also for secret key generation respectively. This system is secure and safe based on standard hardness assumption of Bilinear and DiffieHellman computation.

Index Terms— Bilinear Pairing, Cipher text, Cloud computing, Cloud Service Provider(CSP),Computational DiffieHellman, Elliptical Curve Cryptography(ECC), Identity Based Encryption(IBE),Uni-directional Proxy re-encryption(PRE),

————————————— ◆ —————————————

1 INTRODUCTION

Cloud is the delivery of on demand service, everything from application to data center over the internet on pay for use basis. As we all know cloud provides almost ultimate storage, backup recovery, cost efficient, quick deployment, we cannot deny the fact the data in the cloud is prone to security threat. To avoid this security threat and to provide secure data storage in this system, we focus on Identity Based proxy re-encryption for data storage.

Even though cloud provides lots of services many organizations are reluctant to utilize the facility because of the security issue. This can be overcome by issuing secret key generated based on Identity, and by using unidirectional proxy re-encryption for data storage.

In proxy re-encryption Proxy (CSP) here we are talking can convert an encryption computed under user A's(data owner) public key into an encryption encryption intented for user B(data Storage). In this User A temporily forwarded the encrypted message to User B without sharing the Secret key.

In this work we extended the notion of proxy re-encryption to the area of Identity Based Encryption to secure the data in cloud. In which senders encrypt messages using the recipient's ID(string) as a public key. In this system identity based proxy re-encryption schemes allow proxy (here Cloud Service Provider) to translate an encryption under User A's (data owner) identity into one computed under User B's (data storage) identity, without learning the plain text (data) by using the re-encryption keys.

2 Literature Survey

a) Bilinear Pairing: Let (E, +) and (V,+) denote cyclic groups of prime order q over an elliptic curve. Let P be a generator of E and let e: $E \: X \: E \rightarrow V$ be a bilinear pairing satisfying the following conditions [9],[10],[11]

i) For all points $P, Q \in E$ and for all a,b$\in Z$, we have e(aP,bQ)=e(P,Q)^{ab}

ii) There exist P_1,P_2 $\in E$ such that e(P_1,P_2)$\neq 1$. That is if P is a generator of E then e(P,P) is the generator of V. Such groups may be realized using super singular Elliptic curves and the Weil pairing.[4],[5]

iii) Computing e(P,Q) for all P,Q$\in E$ should be easy.

b) Elliptical Curve Cryptography by Victor Miller and Neil Koblitz [6],[7],[8] as algebraic/geometric entities has been studied for the past 150 years. This ECC generate the key of shorter key length and provides highly secure system.

2.1 Identity Based Encryption:

All organizations are searching for more reliable and stronger authentication methods for their activities. The traditional way of authenticating a person was by PIN and Password which are considered now in this technological world as very less reliable, as these PIN and password are cracked, stolen or lost. Apart from the PIN the identity of a person plays a vital role in the verification process of a signed electronic document or message. Shamir (1984) proposed ID-based encryption and signature scheme to simplify key management procedures in certificate-based public key setting.ID-based public key setting can be a good alternative for certificate-based public key setting. Many ID based Cryptographic schemes were proposed based on bilinear pairings, namely the Weil [4],[5]and Tate pairing of algebraic curves. The secret key will be generated by using the ECC key gen algorithm as it produces the key of minimum key length.

————————————————

i)Ms.S.Jayashree, Senior Lecturer, Department of Computer Science, SriChaitanyaGroupofEducationInstitutions, Bangalore. PH:09538207766 email:jayashree_ananth@yahoo.com

ii) *Dr. R.S. Sankara Subramanian, Professor& Head, Department of Science & Humanities, Kalaignar Karunanidhi Institute of Technology, Coimbatore; PH:07598514912, email: sankarasubramanian.r.s@gmail.com*

2.2 Uni-Directional Proxy re-encryption:

Uni directional proxy re-encryption is a technique used here for data storage, by assigning cloud service provider as a proxy. In this system we extended Ateniese, Fu, Green and Hohenberger [1] proposed an improved, non interactive unidirectional scheme which removed the need for pre-shared keys and permitted arbitrary delegations.

3 Proposed System:

In the proposed System the users of the cloud will obtain the master public key and private key from the trusted third party key generator (PKG)[1]. First User A and User B will obtain the public keys (Q_AID), (Q_BID) after obtaining the public key the key generator will authenticate the Identity of User A and User B, generate the private keys (d_AID),(d_BID). User A now receive and verify the Identity of User B and generate the public key for User B(Q_BID). User A will encrypt the message by using User B public key (Q_BID).The encrypted message will in turn sent to the proxy there the cipher will get re-encrypted by using the re-encrypted key(Q_BID, d_AID). This re-encrypted message will undergo Decrypt scheme where the message will get decrypted by using the decryption key (Q_AID, d_BID).

In the proposed System, in

Step 1 : Trusted Third Party(PKG) will generate the master private and public key. User A, User B will obtain their public keys (Q). PKG will authenticate the users' identity and issue their private key (d).

Step 2: User A uses the identity of User B and generate the public key for User B.

Step 3: The Encryption Algorithm will take the message (m) and User B public key (Q_BID) and encrypt the message.

Step 4: Major drawback in cloud is trusting CSP cent percent. Here we introduced the trusted 3rd party for key generation and key distribution. At CSP, re-encryption takes place for getting cipher text as input. At the client side the first level of encryption is done using the master code of the data storage system. Then a second level encryption using the public key of CSP is done. The multi level encrypted message is received by CSP; here the first level decryption will be done by using with its own key. Now the re-encryption will take place in the CSP will use the re-encryption key given by the receiver.

Step 5: Now the data storage i.e. the receiver decrypts the message using the re-encryption key, followed by the decryption using the master code. Finally the receiver gets the original message. The original data collected is now stored in the data storage.

4 ALGORITHMS:

4.1. Key Generation Algorithm using ECC: [6],[7],[8]

1. Alice selects an integer, d_AID , this is A's secret key (d_AID)
2. Alice then generates a public key
   Q_AID = d_AID * B
3. Bob similarly selects a secret key BSK and computes a public key
   Q_BID = d_BID *B
4. Alice generates the security key
   K = d_AID * Q_BID.
5. Bob generates the secret key
   K= d_BID * Q_AID

4.2. Encryption algorithm:

Suppose A wants to send to B an encrypted message [6],[7],[8]

1. A takes plain text message M, and encodes it onto a point PM, from the elliptic group/
2. A chooses another random integer, k from the interval[1,p-1]
3. The cipher text is a pair of points
   PC= [(kB),(PM+kB_{PK})]
4. Send ciphertext PC to cloud B

4.3. Decryption algorithm:

Cloud B will take the following steps to decrypt cipher text PC [6],[7],[8]

1. B computes the product of the first point from PC and his private key, B_{SK},B_{SK}*(kB)
2. B then takes this product and subtracts it from the second point from PC
   (PM+kB_{PK})-B_{SK} (kB)] =PM+k (B_{SK}B)-B_{SK} (kB)=PM
3. B cloud then decodes PM to get the message M.

5 EQUATIONS

G1- Elliptic curve set
G2- is of order q
P$\in G1$ arbitrary generator, $s \in Z_q^*$
P_{pub} = sp (random master key)
H1:$\{0,1\}^* \rightarrow G_1^*$
H2: G2→{0,1}*

Extract:

$Q_{ID} = H_1(ID)$
$d_{ID} = sQ_{ID}$ (d_{ID} - private key) (1)

Encrypt:

i) $r \in Z_q^*$

ii) $g_{ID}=e(Q_{ID},P_{Pub})$ (2)

iii) $(g_{ID})^{r}$

iv) H2$(g_{ID})^{r}$

v)rp

vi) c=rp||M + H2 $(g_{ID})^{r}$ (3)

Decrypt:

U =rp

V = M+ H2$(g_{ID})^{r}$

M = V + H2(e(d_{ID},U)

e(d_{ID},U) = e(sQID, rp) (4)

=e$(Q_{ID},P)^{rs}$

M+ H2$(g_{ID})^{r}$+n H(d_{ID},U) (5)

=M

6 Helpful Hints

6.1 Figures

Fig- 1 Overview of Proposed System

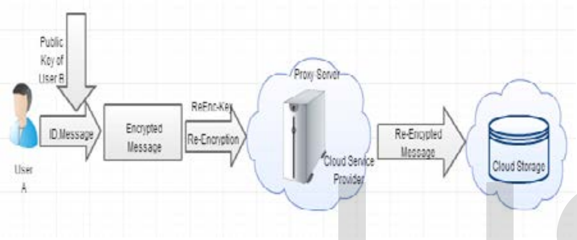


Fig-2 Organizational diagram for Re-Encryption

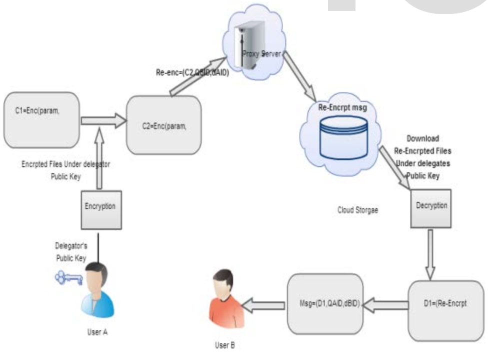
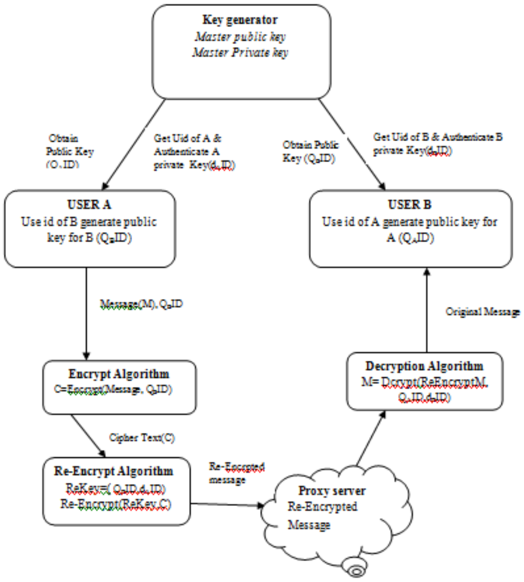


Fig- 3 Organizational diagram of Proposed System



6.2 Notations:

Q_BID= Receiver B's Public Key

Q_AID= Sender B's Public Key

d_AID=Sender A's Secret Key

d_BID = Receiver B's Secret Key

DECRYPT ALGOL=Decryption Algorithm

ENCRYPT ALGOL = Encryption Algorithm

7 CONCLUSION:

In this scheme we will provide of the solution to secure data when the data stored on the cloud using non interactive Identity based uni directional proxy re-encryption. The data on the cloud is re-encrypting by using the key generated by the key generator after authenticating the identity. Hence the data is protected from any modifications or misuse by the unauthorized user, since the service provider cannot review any information which is stored in the cloud as it got re-encrypted. Moreover we are using the identity for generating the key which is the perfect replacement for the certificate. After studying the hardness of the bilinear pairing property we have used computational Diffie Hellman over Elliptical curve, which will produce the minimum key length and this is tough for the unauthorised users. The data in the cloud is secure based on standard hardness assumption of Bilinear and DiffieHellman computation. It works preferably compatible under existing Identity based non interactive proxy re-encryption. By using this methodology we enhance the security of data transfer by introducing the identity based secure encryption and re-encryption. It will provide many advantages like collusion-resistance get the notification of user request on android based device and will also provide security against Distributed Denial of Service attack and it provides secure model of cloud storage with safe data forwarding.

REFERENCES

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green and Susan Hohenber Improved Proxy Re-encrption Schemes with Applications to Secure Distributed Storage. In the 12th Annual Network and Distributed System Security Symposium, pages 29-43, 2005. Full version available at http://eprint.iacr.org/2005/028

[2] Matt Blaze, G. Bleumer, and M. Strauss. Divertible protocolos and atomic proxy cryptography. In Proceedings of Eurocrypt'98, volume1403, pages 127-144,1998.

[3] http://www.di.ens.fr/~vergnaud/publis/ieeetit11a.pdf

[4] Dan Boneh, and Matt Franklin. Identity based encryption from the Wiel Pairing. SIAM Journal of computing, 32(3):586-615,2003.

[5] Dan Boneh, and Matt Franklin. Identity based encryption from the Wiel Pairing. In Advances in Cryptology(CRYPTO 2001), volume 2139 of Lecture Notes in Computer Science pages 213-229. Springer, 2001

[6] Koblitz, N., 1987. Elliptic curve cryptosystems. Mathematics of Computation 48,203-209

[7] Miller, V., 1985. Use of elliptic curves in cryptography. CRYPTO 85.

[8] W.Stallings. Cryptography and Network Security: Principles and Practice (3rd ed.). Prentice Hall, Upper Saddle River, New Jersey, 2003.

[9] Voltage Security,Inc. http://www.voltage.com.

[10] Dan Boneh and Xavier Boyen. Efficient selective-id secure Identity Based Encryption without random oracles. In proceedings of Eurocrypt'04, volume 3027 of Lecture Notes in Computer Science, pages 223-238. Springer, 2004.

[11] Brent Waters. Efficient Identity-Based Encryption without random oracles. In Proceedings of Eurocrypt'05, volume 3494 of Lecture Notes in Computer Science, pages 114-127. Springer,2005.