A Secured Cloud Security Using Elliptic Curve Cryptography

Dr.M.Gobi
Asst. Professor, Department of Computer Science, Chikkanna Government Arts College, Tirupur
Email: mgobimail@yahoo.com
Karthik Sundararaj
Research Scholar, Department of Computer Science, Chikkanna Government Arts College, Tirupur
Email: karthikasundarraj@gmail.com

----------ABSTRACT----------
Cloud Computing is a modern paradigm which enables utilization of pool of computing resources in the most proficient way. This emerging technology provides great opportunity in support of small and medium scale business houses to grow their business using the computing IT resources with no deployment cost. Cloud computing with well-built security has become a boon in the field of Information Technology. Cloud security is becoming a key differentiator and competitive edge between cloud providers. The prime responsibility of the cloud services provider is assuring security and integrity of the consumer's data. The lack of trust on data security is being the key obstacle to the IT sectors to move their data to the cloud. Lot of researches has been done to improve the performance of cloud data security. Hence cloud computing is still discovering several security issues. The high-quality cloud security can be achieved by efficient encrypting techniques. In this paper, we projected a model using Elliptic Curve Cryptography (ECC) to provide efficient data security in Cloud computing.

Keywords – **Cloud Computing, Cloud Security, Elliptic Curve Cryptography, Data Security.**

1. INTRODUCTION

Cloud computing platform is a network of servers and the servers can be physical machines or virtual machines. Cloud computing is a model for enabling convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal effort or service provider interaction. The massive pool of configurable resources in Cloud is available to consumers as service. These services are generally partitioned into three main categories: Software-as-a-Service (Saas), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Cloud Computing has its own attractive characteristics, they are On-Demand Self Service, Broad network access, Resource pooling, Rapid Elasticity and Measured Service. A Cloud Computing environment provides the computing resources based on four major deployment models include Public cloud, Private cloud, Hybrid cloud and Community cloud.

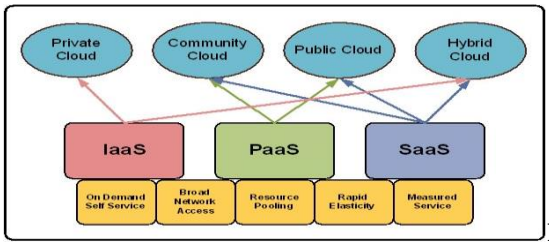

Figure 1

Cloud Computing provides enormous opportunity for small and medium scale endeavors to develop their business using Information Technology services at affordable cost or at no deployment cost. Clouds provide high scalable, durable and flexible services on a pay-per-use method which can be used by the enterprises for enhance their business growth by reducing cost in various ways.

Though Cloud computing has lot of advantages, it still has some challenges which includes privacy and security because it is growing rapidly. As different types of normal data and also secret data are stored in the cloud, the client expects the cloud managing system to protect their data by providing security and maintaining secrecy.

Cloud security can be achieved by cryptography, the science of suppressing information to ensure confidentiality, integrity, privacy, authentication, access control and non repudiation. The major functions of cryptography are encryption and decryption. A well secured cloud is a reliable source to store the data for the enterprises. In general, the cloud data security has some important aspects include availability, data protection, governance, incident response, compliance and identity & access management.

2. REVIEW OF LITERATURE

In paper [8] author considers the cloud environment as a new computing platform to which the classic methodology of security research can be applied. The author determines to employ an attribute-driven methodology to conduct their review. In paper [9] the author analyses the basic problem of cloud's data security. With the analysis of the architecture of HDFS, they get the data security requirements of cloud computing and set up a mathematical data model for cloud computing.

The paper [11] proposed a scheme in which the data are segmented into three different levels according to their data

importance ranking set by data owner. The data in each level can be encrypted by using encryption/decryption algorithms and keys before store them in the Cloud. In this technique the aim is to store data in a secure and safe way in order to avoid intrusions and attacks. Also, it will reduce the cost and time to store the encrypted data in the Cloud Computing.

In paper [12], the authors introduced a proficient model in order to address the problems such as data integrity, data loss and secure data access. It is designed in such a way to provide end – to – end security in the cloud. It helps to assure the data correctness and also helps to simultaneously identify the misbehaving servers in the cloud system. It enables the data owner to have full control of his own data by monitoring the access logs of data file through distributed auditing mechanism. To add more security at the access levels, the data has been converted in a more flexible and scalable form with fine grained access control. Finally the data has been secured at all the levels such as at rest, during transit and access in order to provide a complete end to end security.

In paper [13], the proposed system ensures the corrective measures to protect the integrity of data as well as detecting and preventing possible risks thus ensuring data breaching leading to information leakage is prevented. The system, however, concentrates on mainly information leakage but there are more threats that cloud security faces.

In paper [14], the authors proposed an architecture which can be implemented in cloud environment taking the advantages of linear cryptography for establishing a secure connection and exponential cryptography for encrypting the data. The two algorithms used are Diffie Hellman Key Exchange and Elliptical Curve Cryptography. With help of these two algorithms, the architecture provides a four step procedure for ensuring authenticity of user. The first step is to establish the connection, second is account creation, third is authentication and last one is data exchange. They have used ECC because its computational speed of this algorithm is very less compared to linear algorithms present. One more advantage is that it has a sub exponential time complexity which makes it difficult to crack.

Method proposed in paper [15],

Key generation is an important part where we 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 using its private key. Now, we have to select a number **'d'** within the range of **'n'**.

The public key can be generated by using the following equation:

$Q = d * p$ -------- (1)

where, d = The random number that we have selected within the range of (1 to n-1).

P = the point on the curve.

Q = the public key and 'd' is the private key.

Encryption

Let 'm' be the message which has to be sent. We have to represent this message on the curve. Consider *'m'* as the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].Cipher texts will be generated after encryption, let it be **C**1 and **C**2.

$C1 = k * p$ ----- (2)

$C2 = M + k * Q$ ------ (3)

Decryption

The message 'M' that was sent is written as following equation,

$M = C2 - d * C1$ ----- (4)

Proof

The message 'M' can be obtained back using eq.(4)

$C2 - d * c1 = (M + k * Q) - d * (k * p)$

we have $Q = d * p$, by cancelling out $k * d * p$,

We get M(original message)

3. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group.

For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation:

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

along with a distinguished point at infinity, denoted "∞". (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated). This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

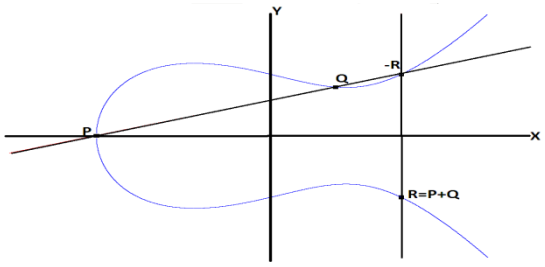

Figure 2

If P and Q are on E, R = P + Q

As shown in Fig.2, Let P=(x1,y1), Q=(x2,y2), R=(x3,y3) and P not equals Q

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

To find intersection with E, we get

$(m(x-x_1)+y_1)^2=x^3+Ax+B$

Or, $0=x^3-m^2x^2+.....$

So, $x_3=m^2-x_1-x_2$

⇨ $y3=m(x_1-x_2)-y_1$

Elliptic curves are used as an extension to other current cryptosystems. ECC is considered as more secured algorithm than other asymmetric algorithms such as RSA and Diffie-Hellman by providing same level of security with smaller key size. For example, ECC can provide a level of security with a 256-bit public key that other techniques require a 3072-bit public key. Thus ECC has some advantages include low CPU consumption, low memory usage and greater speed. The difficulty of discrete logarithm makes ECC so important.

3.1 Elliptic Curve Cryptography (ECC) domain parameters

The public key cryptographic systems involve arithmetic operations on Elliptic curve over finite fields which are determined by elliptic curve domain parameters.

The ECC domain parameters over Fq is defined by the septuple as given below D = (q, FR, a, b, G, n, h), where

- **q:** prime power, that is q = p or q = 2m, where p is a prime
- **FR:** field representation of the method used for representing field elements ∈ Fq
- **a, b:** field elements, they specify the equation of the elliptic curve E over Fq, $y^2 = x^3 + ax + b$
- **G:** A base point represented by G= (xg, yg) on E (Fq)
- **n:** Order of point G , that is n is the smallest positive integer such that nG = O
- **h:** cofactor, and is equal to the ratio #E(Fq)/n, where #E(Fq) is the curve order

The primary security in ECC is the parameter n; therefore the length of ECC key is the bit length of n. For comparative length, the security of ECC keys is much more than that of other cryptosystems. That is for equivalent security, the key length of ECC key is much lesser than other cryptosystems.

4. CLOUD DATA SECURITY USING ECC:

In this proposed scheme, ECC, a public-key cryptosystem is used to generate both private key and public key. For each user two keys will be generated using ECC, first key is called as private key and the second key is called public key. User A encrypts the plain text by using User B's public key and transmits the cipher text in the cloud. User B takes the cipher text from the cloud whenever he needs. Then User B decrypts the cipher text by using his own private key to get the plain text which was transmitted by User A. Since the private key is kept secret, the transmitted data cannot accessed by other persons. In this way the data will be more secured in the cloud.

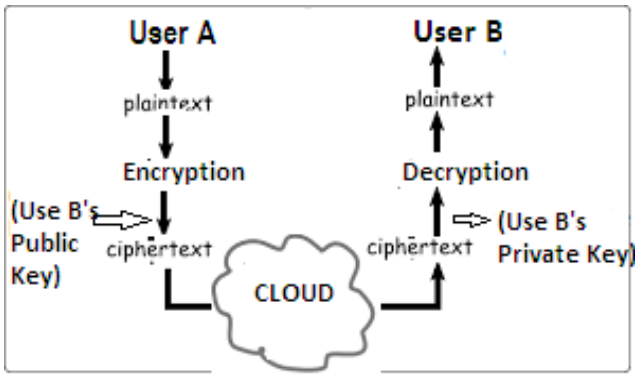

Figure 3

4.1 ALGORITHM FOR CLOUD DATA SECURITY USING ECC:

First of all, the points are generated for the elliptic curve based on the values of prime modulo p and predefined coefficients a, b.

GenPoints (prime, a, b)

```
{
Step 1: initialize x = 0;
Step 2: while (x<p)
        y^2 = (x^3 + ax + b) mod prime;
        if (LHS = RHS)
        output (sqrt (x), sqrt (y));
        x = x+1;
}
```

Algorithm for Key Distribution

```
Step 1: //For user A
        PUB = G*P
        UA = (PUA, PA) // User A key pair
Step 2: // For User B
        PUB = BP*PB
        UB = (PUB, PB) //User B key pair
        // BP is the Base Point
Step 3: //Send the Public key of UB to UA
        Send (PUB, UB);
Step 4: //Send the Public key of UA to UB
        Send (PUA, UA);
```

Algorithm for textEncryption

```
Step 1: Calculate APL = p*AP;
        //p = Ascii value of text
        //AP: random point on EC
Step 2: // Calculate kBP
        kBP = k*BP
        //BP is the Base Point
Step #: // Send Cipher test to receiver, i.e. User B
        Cipher Text, CM = {kBP, APL+ k * PUB}
```

Algorithm for textDecryption

```
Let kBP be the first point
    APL+ kPUB be second point
Step 1: Calculate PBkBP = PB * first_point
```

//this yields us an equivalent point to kPUB
Step 2: Calculate APL = (APL+ k*PUB) - PBkBP
Now using discrete logarithm concept
Step 3: Evaluate value of sent text from APL
APL = rAP
//r is the value to be calculated using the discrete logarithmic concept. r = p, i.e. the original ASCII value.

CONCLUSION

Cloud Computing provides a platform with an enhanced and efficient way to store data in the cloud. The functioning of Cloud Computing is significantly distressed by issues such as that of data security, integrity, theft, loss and presence of infected applications. These issues are the major disadvantages to the consumer to move their data to the cloud. This paper proposed a model using Elliptic Curve Cryptography to enable more efficient data security in the cloud computing. Here, Security is based on the difficulty of computing discrete logarithm in a finite field. El-Gamal and ECC are forms of public key cryptography, in which one decryption key, known as the private key, is kept secret, while another, known as a public key, is freely distributed. Public key cryptography is computationally more expensive than private key encryption, which employs a single, shared encryption key. By using the proposed algorithm, Cloud computing can achieve high level of security more than the security attain by the IT enterprises their own hardware and software.

REFERENCES

[30] Abhuday Tripathi, and Parul Yadav, Enhancing Security of Cloud Computing using Elliptic Curve Cryptography, *International Journal of Computer Applications, 57(1*), 2012, 0975-8887.

[31] Nilesh N. Kumbhar, Virendrasingh V. Chaudhari, and Mohit A.Badhe, The Comprehensive Approach for Data Security in Cloud Computing: A Survey, *International Journal of Computer Applications, 39(18),* 2012, 0975-8887.

[32] N. Koblitz, *Elliptic Curve Cryptosystems, Mathematics of Computation*, 1987.

[33] Yubo Tan, and Xinlei Wang, Research of Cloud Computing Data Security Technology, *978-1-4577-1415-3/12,IEEE 2012.*

[34] Yashpalsinh Jadeja, and Kirit Modi, Cloud Computing - Concepts, Architecture and Challenges, *International Conference on Computing, Electronics and Electrical Technologies,4(12), 2012*, 978-1-4673-0210

[35] Dr. Chander Kant, and Yogesh Sharma**,** Enhanced Security Architecture for Cloud Data Security, *International Journal of Advanced Research in Computer Science and Software Engineering,* 3(5), 2013.

[36] Wayne Jansen, and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, *National Institute of Standards and Technology, U.S. Department of Commerce, 800-144.*

[37] Veerraju Gampala, Data Security in Cloud Computing With Elliptic Curve Cryptography, *International Journal of Soft Computing and Engineering (IJSCE), 2, 2012.*

[38] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, and Tang Chaojing, Data Security Model for Cloud Computing, *Proc. International Workshop on Information Security and Application. Qingdao, China, 2009, 978-952-5726-06-0.*

[39] Ikshwansu Nautiyal, and Madhu Sharma, Encryption Using Elliptic Curve Cryptography Using Java as Implementation Tool, *International Journal of Advanced Research in Computer Science and Software Engineering, 4(1), 2014.*

[40] Vidyanand K\Ukey, and Nitin Mishra, Dataset Segmentation for Cloud Computing and Securing Data Using ECC, *International Journal of Computer Science and Information Technologies, 5(3), 2014, 4210-4213.*

[41] R. Bala Chandar, and M. S. Kavitha, A Proficient Model For High End Security in Cloud Computing, *ICTACT Journal of Soft Computing, 04(02), 2014.*

[42] Nina Pearl Doe, and Sumaila Alfa, An Efficient Method to Prevent Information Leakage in Cloud, *IOSR Journal of Computer Engineering (IOSR-JCE) 16(3), 2014, 2278-8727.*

[43] Neha Tirthani, and Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, *International Association for Cryptologic Research Cryptology ePrint 49, 2014.*