IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. II (May-Jun. 2014), PP 107-112
www.iosrjournals.org

Enhanced Security Model for Cloud Using Ones compliment Re-coding for Fast Scalar multiplication in ECC

Anusha K.P[1], Dr. Pritam Gajkumar Shah[2]
[1]*Student, M.Tech, Computer Science And Engineering, SVCE.*
[2]*Professor, Department of E&C Sri Venkateshwara College of Engineering Bangalore.*

Abstract: *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. With a promising technology like this, it certainly abdicates users' privacy, putting new security threats towards the certitude of data in cloud. The security threats such as maintenance of data integrity, data hiding and data safety dominate our concerns when the issue of cloud security come up. In this research paper, we have contemplated a design for cloud architecture which ensures secured movement of data at client and server end. We have used the non breakability of Elliptic curve cryptography (ECC) with ones compliment for data encryption, proposed algorithm is based on 1's complement subtraction to represent scalar in scalar multiplication which offer less Hamming weight and will remarkably improve the computational efficiency. It has three security checkpoints: authentication, key generation and encryption of data.*

Keywords: *Cloud Computing, ECC, Scalar Multiplication, , One's Compliment, Diffie Hellman*

I. Introduction

Defining cloud computing becomes a difficult task with many definitions, yet no consensus on single or unique on ones. Cloud computing refers to a network of computers, connected through internet, sharing the resources given by cloud providers catering to its user's needs like scalability, usability resource requirements. The US National institute Standards and Technology (NIST) defines it as follows "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Cloud computing allows users to access software applications and computing services. They might be stored off-site at locations rather than at local data centre or the user's computer. Cloud computing caters to users' request for services. There is no need to spend money on purchasing and managing of resources.

In Cloud computing domain, there are set of important policies, which include issues of privacy, anonymity, security, liability and reliability . The most important of these issues is the data security and how cloud providers assures it .Most effective technique to protect our data is its encryption. Different encryption schemes for protection of data have been in use for many decades. Encryption of data is done by converting data from normal plaintext to unreadable cipher text. This tactic, however, doesn't prove to be much effective for cloud systems as this conversion involves huge and very complex mathematical computations.

II. Issues In Cloud Security

The three issues of cloud computing security are: confidentiality, integrity and availability; known as the ACI triad .

A. *Availability*

Availability is the attestation that data will be available to the user in a perpetual manner irrespective of location of the user. It is ensured by: fault tolerance, network security and authentication.

B. *Integrity*

Integrity is the assurance that the data sent is same as the message received and it is not altered in between. Integrity is infringed if the transmitted message is not same as received one. It is ensured by: Firewalls and intrusion detection.

C. *Confidentiality*

Confidentiality is avoidance of unauthorized exposé of user data. It is ensured by: security protocols, authentication services and data encryption services.

Since cloud computing is utility available on internet, so various issues like user privacy, data theft and leakage and unauthenticated accesses are raised. Cryptography is the science of securely transmitting and retrieving information using an insecure channel. It involves two processes: encryption and decryption. Encryption is a process in which sender converts data in form of an unintelligible string or cipher text for transmission, so that an eavesdropper could not know about the sent data. Decryption is just the reverse of encryption. The receiver transforms sender's cipher text into a meaningful text known as plaintext.

III. Problem Statement

The security of data of the user is prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. The related works mentioned above have focused on cloud security issues. They have provided different mechanisms for data security in cloud environment. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. But the complexity of the cryptographic algorithm used, hasn't been given much importance. The complexity of the algorithm directly affects the speed of data access. We need some algorithm that will help in efficient and speedy secured data access.

IV. Elliptic Curve Cryptography Preliminaries

Elliptic Curve Cryptography was introduced by Victor Miller and Neal Koblitz inde- pendently in the early eighties. The advantage of ECC over other public key cryptography tech- niques such as RSA, Diffie-Hellman is that the best known algorithm for solving ECDLP the underly- ing hard mathematical problem in ECC takes the fully exponential time. On the other hand the best algorithm for solving RSA and Diffie-Hellman takes sub exponential time. To sum up the problem of ECC can be solved only in exponential time and so far there is a lack of sub exponential attack on ECC.

An elliptic curve E over GF(p) can be de-fined by y2 = x3 +ax+b where a, b GF(p) and 4a3+27b2 ≠0 in the GF (P). The point(x, y) on the curve satisfies above equation and the point at infinity denoted by is said to be on the curve. If there are two points on curve namely, $P(x_1, y_1)$, $Q(x_2, y_2)$ and their sum given by point $R(x_3, y_3)$ the algebraic formulas for point addition and point doubling are given by following equations:

$$X_3=\lambda^2- X_1-X_2$$
$$Y_{3=} \lambda (X_1-X_3)-Y_1$$
$$\lambda = \frac{Y_2 - Y_1}{X_2 - X_1}, \text{ if } P \neq Q$$
$$\lambda = \frac{3X^2 + a}{2Y_1}, \text{ if } P=Q$$

Where the addition, subtraction, multiplication and the inverse are the arithmetic operations over *GF*(*p*), which can be shown in Figure 1.

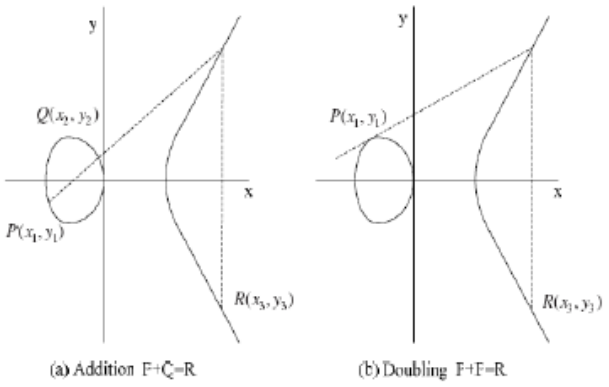

Figure 1. Point addition and point doubling on elliptical curve

V. Recoding Of Integer K In Scalar Multiplication

The number of point doubling and point additions in scalar multiplication depends on the recoding of integer *k*. Expressing integer *k* in binary format highlight this dependency. The number of zeros and number of ones in the binary form, their places and the total number of bit affects computational cost of scalar multiplications. The Hamming weight i.e. the number of non-zero elements, determines the number of point additions and bit length of integer *K* determines the number of point doublings operations in scalar multiplication. One point addition when $P \neq Q$ requires one field inversion and three field multiplications. Squaring is counted as regular multiplications.

This cost is denoted by $1I + 3M$, where the *I* denotes the cost of inversion and *M* denotes the cost of multiplication. One point doubling when $P = Q$ requires $1I + 4M$ as we can neglect the cost of field additions as well as the cost of multiplications by small constant 2 and 3 in the above formulae.

VI. Existing System

Data security is a fundamental mechanism to enable the secure data transmission across the network. There are several mechanism which involved in providing data security across the network.RSA cryptosystem is the existing mechanism used to provide data security. In RSA cryptosystem 1024bit key is used to provide data security. Due to larger size of the key the computational speed of system will decrease. RSA cryptosystem prone to attacks, current research states that RSA encryption can be hacked within 13seconds.

- *The existing methods of scalar multiplication*

1. Binary Method

Scalar multiplication is the computation of the form Q = kP, where P and Q are the elliptic curve points and k is positive integer. This is achieved by repeated elliptic curve point addition and doubling operations. In binary method the integer k is represented in binary form:

$K=\sum k_j 2_j \quad K_j \in \{0.1\}$ The Binary method scans the bits of either from left-to-right or right-to-left.

The cost of multiplication in binary method depends on the number of non zero elements and length of the binary representation of k. If the representation has $k_{1-1} \neq 0$ then binary method require (l - 1) where l is the length of the binary expansion of k and (W – 1) is the Hamming weight of the k that is the number of non-zero elements in expansion of k. For example if k = 629 = $(1001110101)_2$, it will require (W – 1) = 6-1= 5 Point additions and l – 1 =10-1 = 9 point doublings operation.

2. Signed Digit Representation Method

The subtraction has virtually same cost as addition in the elliptic curve group. The negative of point (x, y) is (x- y) in odd characteristics. This leads to scalar multiplication methods based on addition –subtraction chains, which help to reduce the number of curve operations. When integer k is represented with the following form, it is called as binary signed digit representations

$K=\sum S_J 2^j, S_j \in \{1,0\text{-}1\}$

When signed digit representation has no adjacent on zero digits, i.e. $S_{j+1} = 0$ for all $j \geq 0$ it is called non-adjacent from (NAF)

VII.Proposed System

In this paper we aim at removing the security threats for cloud architecture by using two encrypting techniques: Diffie Hellmann Key Exchange and Elliptic Curve Cryptography with one's compliment. To deploy these two methods, we have proposed a new architecture which can be used to design a cloud system for better security and reliability on the cloud servers at the same time maintaining the data integrity from user point of view. Our system involves following steps:

1. Establishment of connection

As soon as the user logs in our system for the first time, he is asked to make an account in the system. The initial connection is established with the help of HTTPS and SSL protocols.

2. Account Creation

For the first time when a secured connection is formed, the user is asked to fill in the account details required for account creation in our cloud system. These details are sent over the internet to our server. The account is created in the system. Further, the connection is then established by Diffie Hellmann Key Exchange protocol. The server also generates the user id which acts as unique user identifier, its Diffie Hellman equivalent stream, required private and public key for ECC encryption. The user id is sent to the user over the secured channel.

User is asked to keep this id as a secret because it is used as a tool to authenticate him every time he logs on to the system.

3. Authentication

As soon as the user opens the home page of cloud server, SSL connection is established. As the account is created, the user is asked to authenticate himself giving all the necessary details and the secret user id sent to him earlier.The cloud server checks the validity of user by first finding out the Diffie Hellman equivalent of the user id from the server repository.If the key matches,then the connection is established by this protocol again and user is logged in to the server. At the back end of user, its private key and the ECC algorithm is sent for encryption.

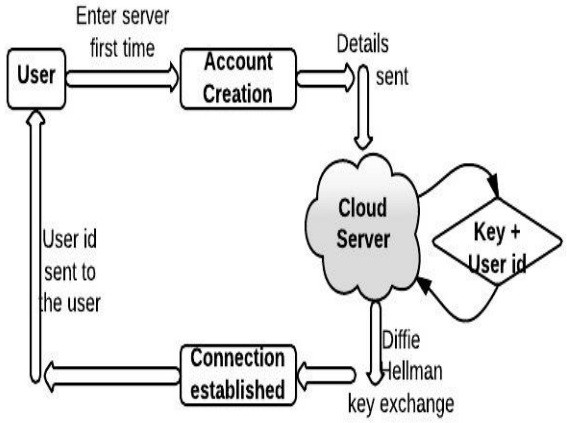

Figure 2: Account creation process

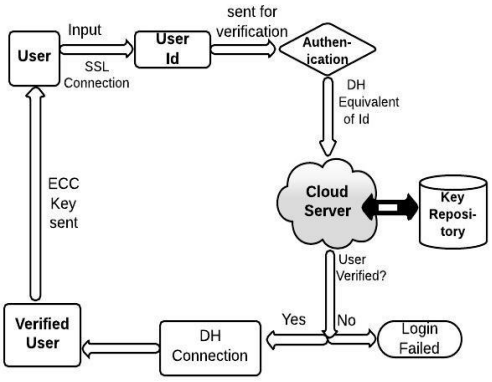

Figure 3: Authentication of user

4. Data Exchange

The data exchange here includes 2 steps:

- The client side: The client wants to fetch a data from server repository; his query is converted in a form of file and encrypted using ECC algorithm. This encrypted data is then sent to server for processing.
- The server side: The server receives the encrypted data. It decrypts it using the private key and processes user query. The result of so obtained is encrypted again and sent to the client side.

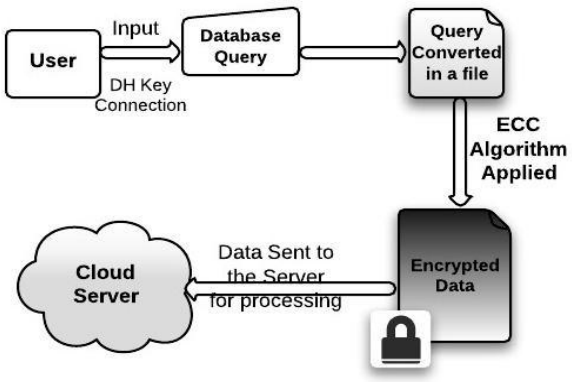

Figure 4: Data Processing view of Client

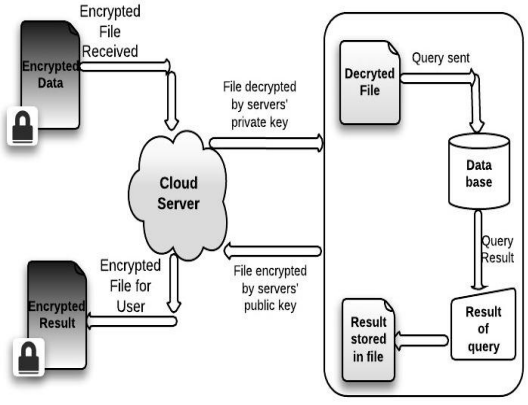

Figure 5: Data Processing view of Server

- *proposed algorithm based on one's complement for recoding of scalar k*

A subtraction by utilization of the 1's complement is most common in binary arithmetic. The 1's complement of any binary number may be found by the following equation :

$C1 = (2a - 1) - N$ (I)

Where, C1 = 1's complement of the binary number

a = number of bits in N in terms of binary form

N = binary number

A close observation of the equation (I) reveals the fact that any positive integer can be represented by using minimal non zero bits in its 1's complement form provided that it is having minimum of 50% Hamming weight. The minimal non zero bits in positive integer scalar are very important to reduce number of intermediate operations of multiplication, squaring and inverse in elliptical curve cryptography as we have seen in the previous sections. The equation (I) can be modified as per below :

$N = (2a – C1 – 1)$ (II)

For example let us take N = 1788

N = (11211111100)2 in its binary form

C1 = 1' s Complements of the number of

N = (00100000011)2

'a' it is in binary form so we have a = 11

After putting all the above values in the equation II we will get ,

1788 = 10000000000-00100000011-1….. (III)

1788= 2048 – 256-2-1-1

As evident from equation III the Hamming weight of scalar N has reduced from 8 to 5 which will save 3 elliptic curve addition operations. One addition operation requires 2 Squaring, 2 Multiplication and 1 inverse operation. In this case total 6 Squaring, 6 Multiplication and 3 Inverse operations will be saved.

The above recoding method based on one's complement subtraction combined gives very good optimization results.

VIII. Computation Of Key For Cryptography

The key generation in this architecture takes place at two levels: one for ECC and other for Diffie Hellman.

1. For ECC

The public key is point on the curve. Private key is a random number. The public key is generated by multiplying private key with generator point G. This point generation and other factors are discussed below.

A. Computation of Point on the Curve

ECC algorithm has the ability to compute a new point on the curve given the product points. We encrypt this point as information to be exchanged between the end users.

B. Choice of Field

To analyze algorithms with smaller computations, we use polynomial time algorithms and for complex computations can be evaluated with exponential time algorithms. The equation of an elliptic curve is given as, $Y2 = x3+ax+b$

C. Integer Factorization

Given an integer n which is the product of two large primes' p and q, we have:

$Y2= x3+ax+b$

It is easy to calculate n for given p and q. It is computationally infeasible to determine p and q for large values of n. Its security depends on the difficulty of factoring the large prime numbers. The method used to solve Integer Factorization problem is the Number Field Sieve which is sub exponential algorithm.

D. Key Generation

Key generation is an important part. An algorithm should generate both a public and private key. The sender will encrypt the message data with the receiver's public key and receiver will decrypt with its private key. Select a number, d in range of n. We generate the public key using following equation,

Q = d*p

d = the random number in range of (1 to n-1). P is a point on curve. Q is public key. d is private key.

E. Encryption

Let 'm' be message to be sent. Consider 'm' has point 'M' on the curve 'E'. Randomly select a value 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be B1 and B2.

B1 =k * P

B2 = M + (k * P)

F. Decryption

Use the following equation to obtain original message that was sent i.e. 'm'.

M = B2 – d * B

M is original data that was sent.

2. Diffie Hellman Key Exchange

This protocol is one of the pioneers in birth of public key cryptography. It follows the following steps.

Input: G is an abelian group; g € G, m is prime multiplicative order.
Output: A secret s € G which will be shared by both the sides.
Steps:

1. Sender generates random d_A € {2,....,m-1} and compute $e_A = g^d$ A.
2. Sender sends e_A to receiver.
3. Receiver generates a random d^B € {2,....,m-1} and compute $e_B = g^d$ B.
4. Receiver sends e_B to receiver.
5. Sender calculates $S = (e_B)^d A = g^d A^d B$
6. Receiver calculates $S = (e_A)^d B = g^d A^d B$

IX. Conclusion And Future Scope

In this paper, we have analyzed the security issues faced by user's private data in the cloud system and the inevitable need to find a solution to the problem. Data security can be very well assured by use of linear cryptographic algorithms but the massive amount of data in cloud computing put a hindrance to the idea. So, we have 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 ones compliment. With help of these two algorithms, we provide 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. We have used ECC because its computational cost 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. We have used Diffie Hellman protocol as it significantly better for establishment of connections. In future, we emphasize on the implementation of the proposed architecture along with different comparisons to show the effectiveness of our proposed architecture.

References

[1] "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography" Neha Tirthani Ganesan R School of computing Sciences and Engineering,School of computing Science and Engineering,M. tech. Computer Science,Associate Professor (CSE),VIT, Chennai campus,neha.tirthani2013@vit.ac.in VIT, Chennai campus,ganesan.r@vit.ac.in

[2] "Algorithm based on one's complement for fast scalar multiplication in ECC for Wireless Sensor Network" Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, University of Canberra, Australia

[3] "Enhancing Security of Cloud computing using Elliptic Curve Cryptography" Abhuday Tripathi MTech Amity University Lucknow , Volume 57– No.1, November 2012.

[4] "Enhanced public auditability & secure data storage in cloud computing", Chakraborty, T.K, Dept. of Comput. Sci. & Eng., Motilal Nehru Nat. Inst. of Technol. Allahabad.

[5] "Data Security in Cloud computing with Elliptic Curve Cryptography" Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, ISSN: 2231-2307, Volume-2, Issue-3, July 2012

[6] "Multi-Agent System Protecting from Attacking in Elliptic Curve Cryptography" Xu Huang, Pritam Gajkumar Shah, and Dharmendra Sharma Faculty of Information Sciences and Engineering, University of Canberra, ACT 2601, Australia.