

Data Security in Cloud Computing Using Elliptical Curve Cryptography

Beibei Du
Mentor: Ming Chow

Abstract

Cloud computing is a network-based service that provide sharing of resources such as virtual machine, storage, network, software and applications etc. It helps to reduce capital costs since that cloud users only need to rent resources according to their requirements and pay the services they use. It is very flexible since users can access its service in any place through intranet. However, a variety of security concerns such as integrity, availability and privacy act as barriers for cloud users to adopt the cloud service. Among all of these concerns, security of of data is key concern holding back cloud adoption for individual or companies. The main purpose of this paper will introduce a method to protect data by using Elliptic Curve cryptography algorithm. We will first have a look at what kind of data security problems now common exist in the cloud, why it happens. Then it will give an introduction about ECC algorithm, how this algorithm works, and using ECC in data security of cloud computing. Finally give a conclusion based on that.

1. Introduction

The cloud in the cloud computing is the set of hardware, software, networks and interfaces that combines together to provide service. In the cloud, end user is able to using a network that connects to the server some location and using a lot of resources. The users don't need to store the data locally. So it reduces the cost of buying hardware, instead of buying the whole framework that just needs to rent the services you wanted according to the personal requirement. Cloud service is responsible to maintain database and applications for end users at remote server and provide independence of accessing the service from any place through the network.

Benefits of cloud computing not only reduce management overhead but also reduce the entrance barrier for new service providers that they can reduce the risk of wasting resources. For enterprises, using cloud service is worthy since in this way, it will bring out lower costs, high profits and more choice. For developers, if using cloud computing, through PaaS model can improve their own capacity. The clouds will grow in size and bring a revolutionary change in the Internet based on its possibility to provide low-cost services.

There are a lot of important issues existed in cloud computing such as privacy, security, integrity, availability and reliability etc. And the most important between all of these is security. But also different end users may have different problems and security requirement. For enterprises, security and privacy is more important and but academia, security and performance are both very important. Nowadays, a lot of encryption algorithms were proposed to improve the security problems. In this paper, it will cover a ECC

algorithm to see how it works and how it can be used in data security problem exists in cloud computing.

2. To the community

2.1 Reason to choose data security topic

As many companies move their data to the cloud, data security becomes the first problem, and cloud data security depends on more than simply applying appropriate data security countermeasures. There are many challenges to overcome. Inappropriate access to customer sensitive data by personal is a potential threat to cloud data, assurances should be provided to the clients and some privacy policies should be in place to assure the cloud users of data security, which related to privacy problem. The cloud provider should also make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place, for compliance purposes, it is necessary to have exact records as to what data was placed in a public cloud, where it was processed, these are related to data integrity problem. Cloud computing offers a high degree of data mobility and users may don't always want to know where their data was stored, but enterprise with sensitive data, they may want to know the location of data and wish to specify a location, in this situation, cloud provider should provide data location to the enterprise and should provide robust authentication to safeguard user's information. Data availability becomes a big issue since customer data is stored in different servers of different locations.

2.2 Why cryptography helps and common cryptography algorithms

Cryptography is the technology of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting plaintext data by taking user data into cipher text. Cryptography is used to provide data integrity, confidentiality etc.

With respect to cloud computing, cryptography can help to resolve security problem in some extent. Security algorithms can be classified as Symmetric algorithms, Asymmetric algorithms, signature algorithm and Hash algorithm etc.

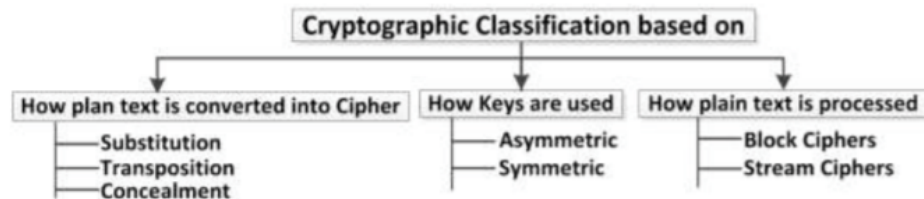


figure 1

Asymmetric algorithm is to use a pair of related key, one key for encryption called public key, another different key for decryption called private keys when performing transformation of plain text into cipher text. ECC, RSA and Diffie-Hellman are main asymmetric algorithms.

Symmetric algorithm uses one single shared secret key to encrypt as well as decrypt data and is capable of processing large amount of data. Symmetric algorithms encrypt plaintext as Stream ciphers bit by bit at a time or as Block ciphers on fixed number of 64-bit units.

3. Elliptic Curve Cryptography Background

ECC cryptography is an approach to public-key cryptography using the elliptic curves. It uses smaller keys and is faster than RSA in some extent, although it has almost same level of security. ECC is based elliptic curve discrete log problem, and it's a much harder problem than factoring integers. ECC relies on the difficulty of solving the discrete logarithm problem for the group of an elliptic curve over some finite field as like integers module a prime number. Elliptic curves have cryptographic value because a user can 'multiply' a point by a number to produce another point on the curve, but cannot easily figure out what number is used. First, use mathematical operations to map the plaintext message to a point on elliptic curve, and to get the cipher text, it's also needs to use elliptic curve operations.

What's elliptic curves? An elliptic curve over real numbers is a set of points (x, y) satisfies equation $y^2 = x^3 + ax + b$, a, b, x and y are real numbers and elliptic curve changes with various choices of a and b . If have two points P and Q on an elliptic curve, how do we perform addition operation to determine point R which equals $P + Q$, the point is that draw a line through P and Q , this line will intersect on the elliptic curve at a third point, then reflect this point via axis- x to get point R , as shown in figure 2 below.

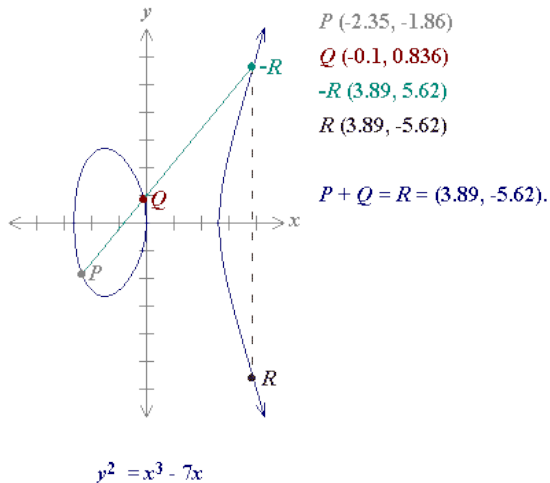


figure 2

Two exceptions exist when drawing a line through points P and Q. First is when adding points P and $-P$, the second is when doubling point P. In the first case, drawing a line through point P and $-P$ will result in a vertical line which means that it won't have an intersection point in the elliptic curve, so the point at infinity O. In the doubling point situation, which also means add point P to itself, a tangent line to the curve is drawn at the point P, this line will intersect on the elliptic curve at the point $-R$, then reflected into axis-x to get point R, example will be like figure 3, and figure 4 shows that if y value of point P is zero, then $2P = O$

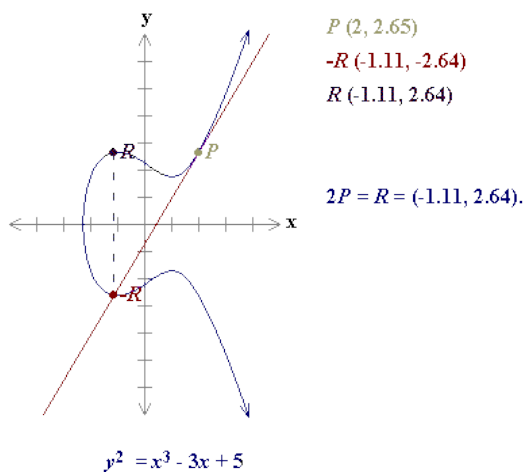


figure 3

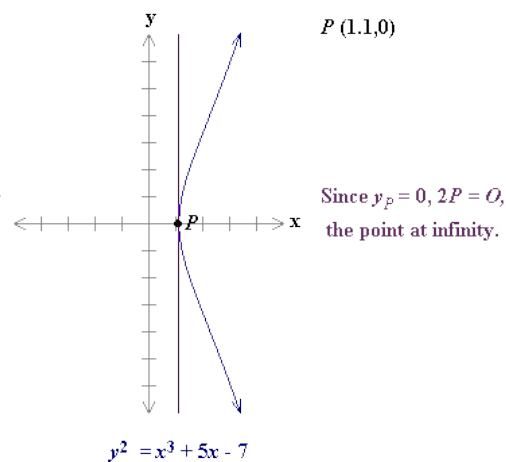
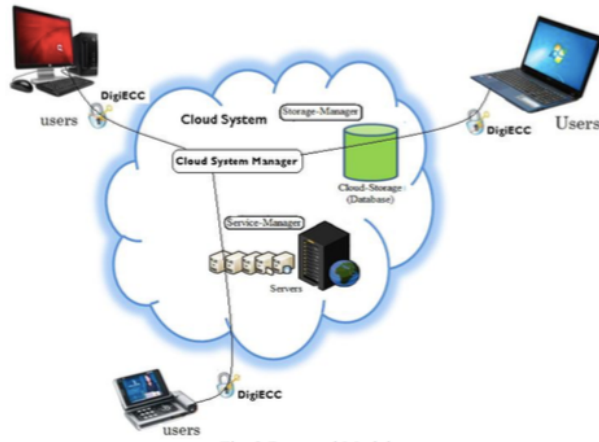


figure 4

Mathematical calculations on elliptical curves may be a little complicated. For example, point $P = (x_1, y_1)$, point $Q = (x_2, y_2)$, addition of P and Q is point $R(x_3, y_3)$. Using equation $y^2 = x^3 + ax + b$, we can get $x_3 = (s^2(x_1 - x_2) - y_1)(\text{mod } p)$ and $y_3 = (s(x_1 - x_2) - y_1)(\text{mod } p)$, s is value of slope and $s = (y_2 - y_1)/(x_2 - x_1)$ if P and Q is different, $s = (3x_1^2 + a) / (2y_1)$ if P equals Q , p is prime number here. But we also should realize that it's just because the complicated math calculation that makes system more secure.

4. Algorithms for data security using ECC

Assume we have two organizations A and B . A and B act as public clouds with data, software and applications. A want to send data to B 's cloud securely and data should be authenticated. Here we can use digital signature and encryption to data with ECC in order to send secure data from A to B . Suppose B wants a document from A 's cloud, B 's user will initialize a request to A 's user, A 's user select the corresponding document from A 's cloud data storage and then apply hash function, it will give message digest. Sign the message digest with his private key by A 's software. It is called digital signature. Encrypt digitally signed signature with B 's public key using ECC algorithm. Encrypted cipher message will be send to B . B 's software decrypt the cipher message to this document with his private key and verify the signature with A 's public key.



We assume both A and B agree to some public-known data item:

- The elliptic curve equation: $y^2 = x^3 + ax + b$, where $4a^3 + 27b^2 \neq 0$
- The elliptic group computed from elliptic curve equation
- A, B taken from the elliptic group

Then we have some algorithms for data security using ECC

- Key generation
 - I. A selects random integer d_A , which is A's private key
 - II. A generates a public key $P_A = d_A * B$
 - III. B selects a private key d_B and generates a public key $P_B = d_B * B$
 - IV. A generates the security key $\text{Key} = d_A * P_B$
 - V. B generates the security key $\text{Key} = d_B * P_A$
- Signature Generation
 - I. For signing a message m by sender of cloud A, using A's private key d_A
 - II. Calculate $e = \text{HASH}(m)$, where HASH is a cryptographic hash function, such as SHA-1
 - III. Select a random integer k from $[1, n-1]$

IV. Calculate $r = x_1 \pmod n$, where $(x_1, y_1) = k * B$. If $r = 0$, go to step III

V. Calculate $s = k^{-1}(e + d_A * r) \pmod n$. If $s = 0$, go to step III

VI. The signature is the pair (r, s)

VII. Finally, send signature (r, s) to B

- Encryption algorithm

Assume A send an encrypted message to B

I. A takes plaintext message m , and encodes it onto a point, p_m , from the elliptic group

II. A chooses another random integer, k from interval $[1, p-1]$

III. The cipher text is a pair of points $p_c = [(k*B), (p_m + k * P_B)]$

IV. Send cipher text p_c to B

- Decryption algorithm

B will decrypt cipher text p_c

I. B computes the product of the first point from p_c and its private key d_B , which is $k*B * d_B$

II. B takes this product and subtracts it from the second point from p_c , $(p_m + k * P_B) - k*B * d_B$, since $P_B = d_B * B$, so the difference is p_m

III. Finally, B decodes p_m to get the message m

- Signature Verification

If B wants to authenticate A's signature, B must have A's public key p_A

I. Verify that r and s are integers in $[1, n-1]$

II. Calculate $e = \text{HASH}(m)$, where HASH is the same function used in the signature generation

III. Calculate $w = (s - 1) \% n$

IV. Calculate $u1 = e * w \% n$ and $u2 = r * w \% n$

V. Calculate $(x1, y1) = u1 * B + u2 * PA$

VI. The signature is valid if $x1 = r \% n$, otherwise invalid

5. Application

Reference paper [10] proposed a cloud architecture using Diffie-Hellman Key exchange and ECC to build a secure cloud system which include four steps.

- Step1: Establishment of connection

User is asked to make an account when login to the system. And initial connection is established with the help of HTTPS and SSL protocols.

- Step2: Account Creation

The connection is established by Diffie Hellmann Key exchange protocol. The server generates the user unique id as user's identifier, its Diffie-Hellman equivalent system, required private and public key for ECC crypton.

- Step3: Authentication

As soon as the user opens home page of cloud server, SSL connection is build. If user wanted to login, first cloud server will make validation of user id from server repository, if matches, login successfully. And at the back end of user, its private key and the ECC algorithm is sent for encryption.

- Step4: Data Exchange

From client side: If user wants to fetch data from server, his query is converted in a form of file and encrypted using his public key. Then encrypted data is sent to user.

From Server side: The server receives the encrypted data. It decrypts using private key and process user query, then encrypted again and sent to client side.

6. Conclusion

Security is recognized as one of the most complex problems as like confidentiality, integrity and authorization in cloud computing. In this paper, we provide an introduction about Elliptic Curve and have a look at the algorithms used with Elliptic Cryptography in data security. In the end, give a simple view to see the cloud architecture established using Deffie Hellman and ECC algorithms. In the future, should see more examples how the ECC algorithms was used and try to build a better application method.

7. References

- 1) <http://askcypert.org/sites/default/files/on%20technical%20isssues%20in%20cloud%20security.pdf>
- 2) <http://cs-www.cs.yale.edu/homes/dna/papers/abadi-cloud-ieee09.pdf>
- 3) <http://www.sciencedirect.com/science/article/pii/S0167739X10002554>
- 4) <https://www.math.hmc.edu/~ursula/teaching/math189/finalpapers/elaine.pdf>
- 5) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.303.2584&rep=rep1&type=pdf>
- 6) http://www.ijirce.com/upload/2014/may/4X_DataSecurity.pdf
- 7) http://www.academia.edu/6721467/Enhancing_Security_in_Cloud_Storage_using_ECC
- 8) <http://www.ijana.in/Special%20Issue/file31.pdf>
- 9) <https://eprint.iacr.org/2014/049.pdf>
- 10) <https://pdfs.semanticscholar.org/99be/06702304b4d9bf2ce1605e7e6e209a6a6886.pdf>
- 11) <http://www.certicom.com>