IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

ISSN: 2664-9519 (Online); Vol. 1, Issue 1, August 2019

Data Security in Cloud Computing Using Elliptic Curve Cryptography

Imran A. Khan and Rosheen Qazi

Department of Computer Science, Bahria University, Islamabad, Pakistan

* Corresponding Author: Imran A. Khan; imranahmadani@gmail.com

Received 10-May; Revised 25-June; Accepted 15-July; Published 15-August

Abstract: Encryption helps in transmitting sensitive data over an insecure channel without any danger of data being lost or being manipulated by some unauthorized entity. Different Encryption schemes have been applied for Data security in a different environment. Many cryptosystems worked during different eras and evolved accordingly with time. This paper mainly focuses on asymmetric encryption which is also known as Public key encryption scheme or Holomorphic encryption. However, due to large key size asymmetric encryption is mostly used for Key exchange rather than data Encryption. Nowadays, Data security is the main issue in large data centers and Cloud computing. This paper uses Elliptic Curve Cryptography to encrypt data in the cloud environment because the size of the key used in Elliptic Curve Cryptography is very small. Due to the small key size of Elliptic Curve, computational power is reduced and this results into least energy consumption. This paper shows that elliptic curve cryptography is fast and more efficient for data protection in a cloud computing environment and reduces the computational power and also increases the efficiency.

Keywords: Data security, RSA, Discrete Logarithm Problem (DLP), Generalized DLP, Elliptic Curve Cryptosystem (ECC), Cloud Computing

1. Introduction

Nearly all cryptosystems are based on complex mathematical operations. The symmetric encryption scheme is based on the single key (Secret Key) with simple mathematical operations like substitution and permutations while Asymmetric encryption involves either factoring large prime numbers (RSA) or it is based on discrete log problems (DLP). The public key encryption scheme is also known as a holomorphic cryptosystem. Key size matters a lot in Public key encryption. Due to this large key size, asymmetric Encryption requires lots of computational power. Modern-day cryptosystems are using Hybrid encryption schemes that is, Asymmetric encryption for Key exchange and symmetric encryption for data encryption. Elliptic curve encryption has solved the problem of large key size. ECC uses small key size to reduce the computational power and this can be implemented in a cloud environment or Wireless sensor networks [1, 2] or smart devices. In cloud computing, many users store a large amount of data in a cloud environment. So there are many issues related to data security, privacy, confidentiality, integrity, and authentication. Most of the cloud service provider stores data in plaintext format and user need to use their encryption algorithm to secure their data if required. The data needs to be decrypted whenever it is to be processed.

Different Encryption schemes have different problems this paper discusses the problems with existing encryption schemes and also proposes Elliptic curve encryption for Cloud computing. The paper will elaborate on the process of Elliptic curve encryption scheme. At the end comparison analysis will be done using mathematical modeling or via a simulation [3].

Cloud computing is a new term in information technology in which resources are being shared on the distributed environment over the internet for different purposes like storage and application development. In a cloud environment, users are working over the internet for applications development, data storage. There are three main applications of cloud computing. Software as service means software applications deployed over the internet which can act as Service provider to end-user. Other includes Platform as Service and Infrastructure as Service. Since data is being stored online, so data security becomes the main issue. In a cloud environment, the security model is based on three types of security operations which are 1.Key generation 2. Encryption of data 3. Decryption. For this data security Purpose, different encryption algorithms can be used.

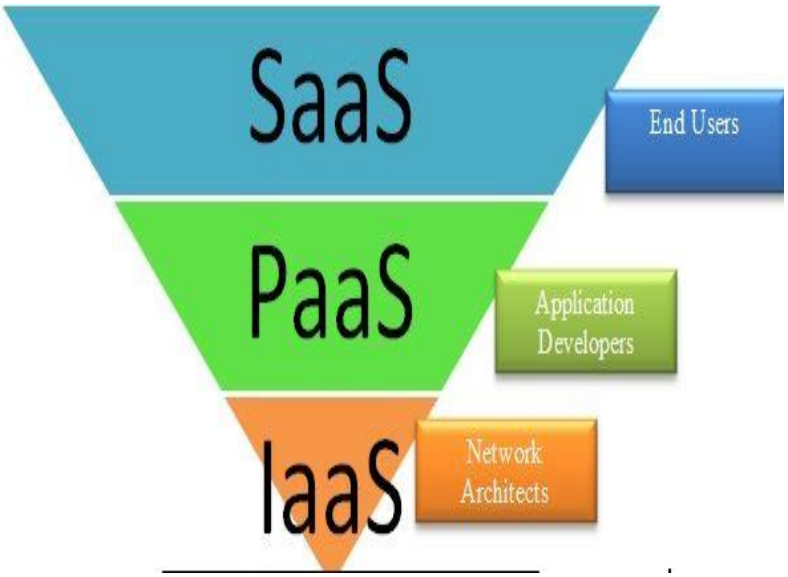

Figure 1. Cloud Computing Applications

Figure 1 shows the cloud computing environment. Saving data in a cloud environment is beneficial in terms of storage management but the issue of data security arises as data is available on online servers. Anyone can have access to data if it is not properly secured on the cloud server. Currently, a trust-based model is implemented in such a way that user and client should rely on the service provider. An efficient and secure encryption scheme is required to secure and save the date in a cloud environment. Here in this paper, a model has been proposed to store data on multiple servers in such a way that encryption and authentication are ensured by using that proposed model.

2. Related Work

In this section, we analyze a Public key cryptosystem and how elliptic curve works on prime fields. Asymmetric Encryption is based on modular arithmetic and DLP. RSA is the most widely used public-key cryptosystem and it is based on integer factorization [4] which is one-way function. One way functions are those which easy to solve in one direction but could not be reversed or very difficult to solve backward. Other Cryptosystem like Elgamal Scheme, Diffie–Hellman, and ECC involve groups and Rings. Cyclic groups are used to create generators of elements of sets. For example, let us take the example of Z^*11. Order of Group Z*11 is 10. Now let us calculate the order of element let us say "a" is 2. We will perform group operations to find the identity element.

$a^1 = 2 \mod 11$ $a^2 = a^{1.} a^1 = 4 \mod 11$

$a^3 = a^{2.} a^1 = 8 \mod 11$ $a^4 = a^3.a^1 = 5 \mod 11$

$a^5=a^4.a^1=10 \mod 11$ $a^6=a^5.a^1=9 \mod 11$

$a^7=a^6.a^1=7 \mod 11$ $a^8= a^7.a^1=3 \mod 11$

$a^9= a^8.a^1=6 \mod 11$ $a^{10}= a^9.a^1= 1 \mod 11$

So a=2 is primitive element and generator of all elements of Z*11 group elements. Please note that Z*11 ={1,2,3,4,5,6,7,8,9,10}. These groups are the basis for discrete logarithm cryptosystems.

A. Elliptic Curve Cryptography

A different algorithm like Euler's phi function and Euclidean algorithms are used to find the inverse of elements in the sets. The generators or Primitive elements are the elements of a set whose order [E] is equal to the order of Group [G]. The modern-day cryptosystem usually uses hybrid encryption in which keys are exchanged via asymmetric encryption while data encryption takes place by using symmetric encryption like AES or 3DES cryptosystem. ECC -Elliptic Curve Cryptography was independently proposed byGampala, et al. [5] and by Victor Miller in 1985 [6].

ECC uses the concept of Generalized Discrete logarithm Problem (GDLP) in which group operation is not limited to multiplication [4, 7]. For the elliptic curve, the size of the key is small as compared to other Public key encryption. Smaller key encryption schemes take less computational power and are easy to process [8].

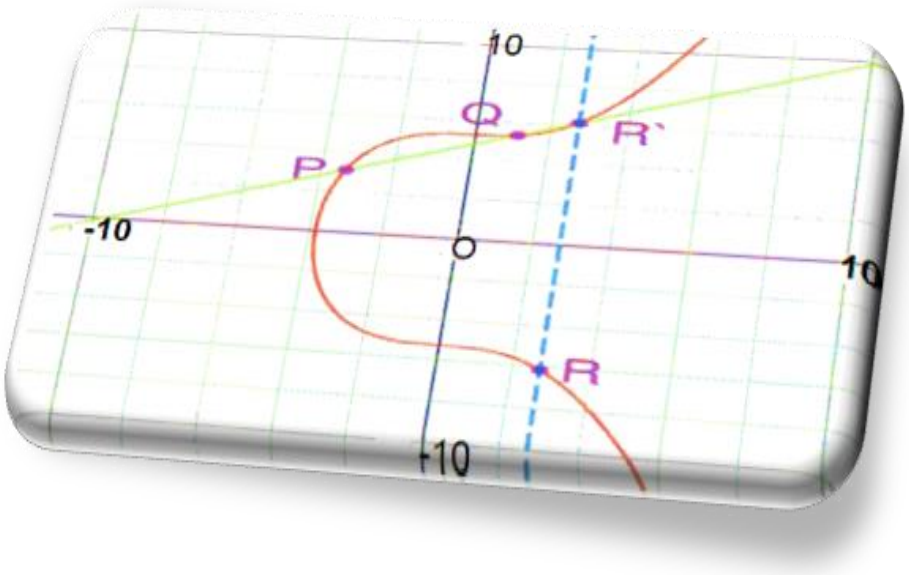

Figure 2. Graphical Representation of points on Elliptic curve

Due to the smaller key size, it helps in energy saving [9]. Mathematical representation of Elliptic Curve is as below.

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

If points are drawn on Elliptic Curve in such a way that line passes through two points on the curve which is shown in Figure 2. Where R- is a reflection of R [8, 10].

The elliptic curve fulfills all four properties of a group. If we add points on an elliptic curve it holds for identity, inverse, closure, associativity and also holds commutative property. It means the Elliptic curve forms an abelian group under addition.

The properties include if a line intersects two points, it will intersect the third point. And if a line is a tangent to the elliptic curve, it will intersect another point on the curve. Table 1 shows a comparison of Elliptic Curve security and RSA Security based on their key size.

Table 1. Comparsion of Key Size in RSA and ECC

ECC(Key Size in bits)	RSA(Key Size in bits)	Key Size Ratio
160	1024	1:6
256	3024	1:12
384	7680	1:20
512	16360	1:30

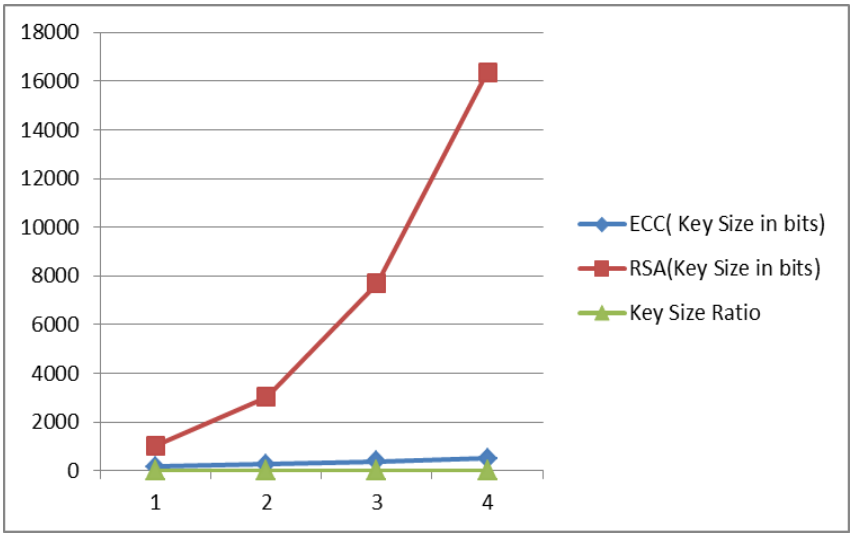

Figure 4. Graphical Representation of Key Size, ECC VS RSA Security on the basis of Key Size

B. Group operations on Elliptic Curve

"+" is group operation on two points on Elliptic curve with X and Y Coordinates.
Let P=(X1, Y1) and Q=(X2, Y2) we need to obtain R.
R = P+Q
R=(X3, Y3)
(X1, Y1) + (X2, Y2) = (X3, Y3)
Here we are adding points not adding numbers. This is geometric interpretation

Point Doubling means addition of same point to get new point in such a way that P+ P where P=Q Hence R = P+P =2P
Point addition means adding two different such that P + Q where P and Q are not equal, So R = P + Q
$X_3 = S^2 - X_1 - X_2 \mod P$
$Y_3 = S(X_1 - X_3) - Y_1 \mod p.$
Where

$$S = \frac{Y_2, Y1}{X_2 - X_1} \mod p \text{ if } P \neq Q$$

$$S = \frac{3X^2_1 + a}{2Y_1} \mod p \text{ if } P = Q$$

Here "S" is the slope of the line. There is a theorem which states that on elliptic curve these points form cyclic groups under some conditions. Elliptic curve discrete logarithm problem (ECDLP) is finding integer s, where $1 \leq s \leq \#E$ such that P+P+…. +P = sP=T where #E shows several unique points on Elliptic Curve. Here "s" is the private key. In ECC "s" is the private key which can be any integer while Public key will be "T" where T is a point on Elliptic curve and is scaler quantity. While in the previous cryptosystem like in "Z*p" keys were integers.

C. Diffie Hellman Key Exchange with Elliptic Curve

1. Choose a point "P" which is prime and elliptic curve.
2. $E=y^2 \equiv x^3 + ax + b \bmod p$
3. Choose a primitive element $P=_{(xp,yp)}$ where p is point on elliptic curve

Alice	Bob
Choose private key	Choose private key
K_{prA}= a Є { 2,3,4……#E}	K_{prB}=b Є { 2,3,4……#E}
Compute K_{pubA}= aP = A = (X_A, Y_A)	Compute K_{pubB}=bP = B =(X_B,Y_B)
Alice send its Public Key to Bob ⇢	
	A
⇠	Bob send its Public key to Alice
B	
Compute aB=T_{AB}=(X_{AB} , Y_{AB})	Compute bA=T_{AB} = (X_{AB} ,Y_{AB})

3. Proposed Scheme

ECC is based on prime fields or the binary extension in the Galois field. It is very difficult to break ECC cryptosystem because it is difficult to find a relation between P and Q the points on Elliptic curve. In this paper, ECC is used for encryption, key generation, and decryption. Selection of Point P(x, y) is very important in developing a secure and more reliable encryption scheme. This paper suggests two-layered approaches to secure data in a cloud environment. One is dividing the data into small parts and secondly choosing random secure curves for encryption. The two steps will ensure data security in such a way that quantum computer system may not be able to break data security. As dynamic elliptic Curve system is being selected for data encryption.

The first step to store data in cloud computing is just to divide the data into 5 data packets. Along with these 5 data packets add 4 bits 0000(1), 0001(2), 0010(3), 0011(4), 0100(5). These 4-bit data can be randomly added to data Packets. Secondly, Elliptic curves with different key sizes are chosen to encrypt the data in a cloud environment. So the parameters for Elliptic curve are chosen from a set of already selected secure Curves. The key size proposed for encryption is small so that computational power should be minimized. This random selection of curves will help to secure data in many ways. Data security is based on two factors. One is dividing the data into small parts with the addition of four bits and the second one is choosing multiple elliptic curves with different points like (P0, P1, P2, P3….Pn-1) for encryption of that data. This will ensure to secure data as two operations are being performed on data simultaneously. Previously presented papers were only dividing the data packets into small segments and were using the same ECC for all data segments [2]. Dynamic key assignment is the most difficult thing which hardened the algorithm used in this proposed scheme. Random number generator is used to generate points of Elliptic curve within a given range. Whenever the request is generated to encrypt data, a set of parameters are provided by using these random number. ECC configurable library named as MoTE elliptic curves [11] was developed by Liu et al using lightweight elliptic curve family.

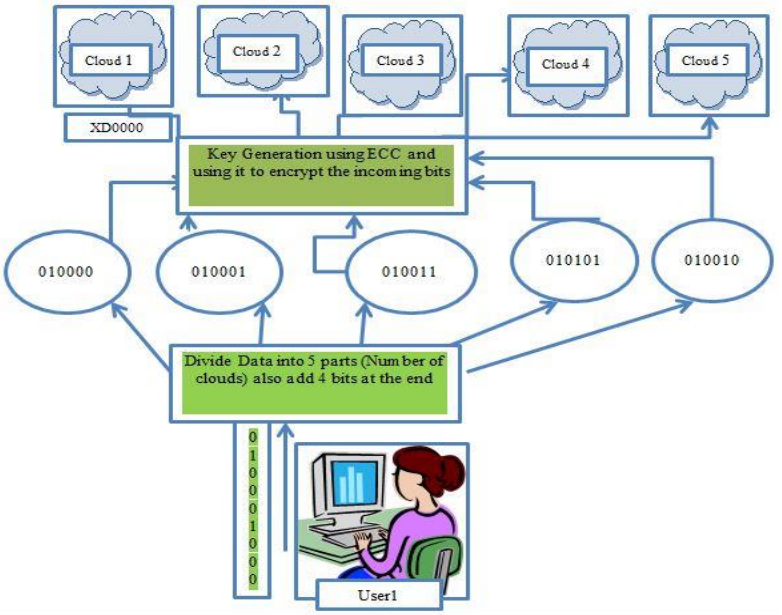

Figure 3. Data Storage Model in Cloud computing

4. Results and Analysis

The proposed algorithm was run alongside RSA, for the same setup RSA and ECC were compared. It is observed that ECC outperforms RSA and is much faster as compared to RSA [10]. The security level achieved using elliptic curves, is far better than RSA [12].

Table 2. ECC VS RSA Performance analysis

Parameters	**ECC**	**RSA**
Computational overheads	Approximately 10 times lesser than RSA	More
Key Size	Key Size is small	Key Size is large
Bandwidth savings	More bandwidth savings	Less bandwidth savings
Key Generation	Faster	Slower
Encryption	Faster	Slower as compared to ECC
Decryption	slower	Faster

5. Conclusions

Cloud computing is emerging as the latest model for data communication. Many Crypto-Algorithms are available for encryption of data in cloud architecture such as symmetric-key cryptography like AES, DES and Triple DES where a single key is used for encryption and decryption while in case of asymmetric cryptography like RSA, ECC and Elgamal, pair of keys (Public and Private Keys) are used. Asymmetric cryptosystems are relatively less vulnerable to attacks and are mostly used for key management purpose. The most significant algorithm in a public-key cryptosystem is RSA which uses comparatively larger Key size than ECC. In this paper, we have tried to analyze the efficiency of ECC which are shown in Table-1 and Table-2. ECC can also optimize memory space as well as reduce the computational complexity which will result in low energy consumption for smart devices. So ECC is also recommended for smart devices as well. Using ECC in cloud computing is more reliable and efficient until quantum computers are not available in the market. Quantum Computer can break the elliptic curve Cryptosystem. However, future work is required for further exploring the storage management

in a cloud environment using ECC. In the future, the proposed model may be implemented in some way or may require some modification to store data in a cloud environment.

References

[1] K. Khan, "The Security of Elliptic Curve Cryptosystems-A Survey," *Global Journal of Computer Science and Technology*, 2015.

[2] A. Chhabra and S. Arora, "an elliptic curve cryptography based encryption scheme for securing the cloud against eavesdropping attacks," in *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, 2017, pp. 243-246.

[3] M.-Q. Hong, P.-Y. Wang, and W.-B. Zhao, "Homomorphic encryption scheme based on elliptic curve cryptography for privacy protection of cloud computing," in *Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on*, 2016, pp. 152-157.

[4] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*: Springer Science & Business Media, 2009.

[5] V. Gampala, S. Inuganti, and S. Muppidi, "Data security in cloud computing with elliptic curve cryptography," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, pp. 138-141, 2012.

[6] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, 1985, pp. 417-426.

[7] A. A. Ibrahim, W. Cheruiyot, and M. W. Kimwele, "Data Security in Cloud Computing with Elliptic Curve Cryptography," *International Journal of Computer (IJC)*, vol. 26, pp. 1-14, 2017.

[8] D. Toradmalle, S. B. Ingale, M. G. Chaudhary, A. V. Aishvarya, and A. R. Patil, "A Survey of Different Encoding Schemes for Improving the Efficiency of Text based Cryptosystem using ECC," *International Journal of Computer Applications*, vol. 153, 2016.

[9] T. Banerjee and M. A. Hasan, "Energy efficiency analysis of elliptic curve based cryptosystems," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1579-1583.

[10] C. Varma, "A Study of the ECC, RSA and the Diffie-Hellman Algorithms in Network Security," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1-4.

[11] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proceedings of the 7th international conference on Information processing in sensor networks*, 2008, pp. 245-256.

[12] J. Athena and V. Sumathy, "Survey on Public Key Cryptography Scheme for Securing Data in Cloud Computing," *Circuits and Systems*, vol. 8, p. 77, 2017.