Secure Communication in Cloud by Using ECC Algorithm

Kamyab Khajehei

Computer Science (Mathematics Department), Under faculty of Science College, Osmania University, Hyderabad, India.

Abstract

Nowadays with the epidemic use of the cloud computing global applications, enterprise companies with large and medium scale are going forward to replace their traditional computer infrastructure to the cloud infrastructure system with the lowest cost. Hence the risk of linking their data also raise to the upper level and security level also needs to be increased.

The cloud computing you do not have a control on the location of VM that you are using it and various users will be present which called as multi-tenancy and some of them might be the black hat hackers. We might face a lot of challenges that can make the cloud environment unsecure.

One of the security risks is communication between two VMs. We suggested the Elliptic-Curve-Cryptography which provides more security level with the least key length, in the way of finding a robust replacement for the current public key cryptography like RSA.

1. Introduction

The cloud computing is the internet base technology which developed with help of virtualization technology. The cloud computing is used the virtualization and VMs [1] and you do not have a control on the location of VM that you are using it. It could be physically located anywhere and anyone can be your neighbor VM [2]. Therefore, communication between cloud service provider and the cloud users will be via the internet channels and it means whole data packets move across the network between cloud users and the cloud infrastructure and the security threat shadows on this type of communication. On the other hand, supporting multi tenancy which several enterprises which store their data in single virtualization based server and sometimes different multiple operating systems are running in single virtual server and may need communication between VMs for message passing purposes in virtualization base cloud computing environment could be threatened by other VMs in same cloud infrastructure.

In both cases, especially in public cloud environment, there are different risks and threats which need the confidence of users like e-banking organizations that highlights the importance of cryptography in their communication channels.

There are different algorithms which can be used for secure communication such as conventional public key cryptography [3], but the problem with traditional cryptography algorithms like RSA is the length of the key and as NIST mentioned the RSA with 1024 key length is not secure anymore [4]. Therefore, it needed to increase the key length which makes a serious problem for key management systems. Hence we must find the replacement for the traditional cryptography algorithms to increase the security of communication in a cloud environment with less key length and higher level security.

There are some public key cryptography algorithms which are candidate to use for secure communication and one of them is Elliptic-Cure Cryptography (ECC) [5].

Elliptic-Cure Cryptography use very small size key compared to the algorithm like RSA, and provide more security, this article we discuss about why we prefer the ECC algorithm for secure communication and its basics.

2. Secure communication between cloud infrastructure and cloud users

In the cloud environment which is kind of distributed network, there are different devices with different capacity of memory, processor and storage as cloud clients. They are various devices from thick and thin client to laptop and Smartphone [6]. In most of the time they are using unsecure LANs and exponentially wireless network which makes client side of cloud environment unsafe and easy to sniff. Hence we need robust cryptosystem with high security and also concerning about the limitation of the clients. The elliptic-curve cryptography is the one of the algorithm that is suitable for these types of clients.

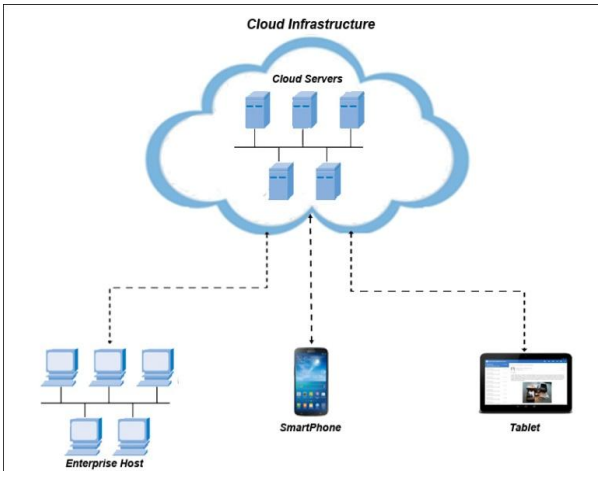

Figure 1: Cloud Network

The main issue is about key management, the comparison which is done by NIST [4] shows that the elliptic-curve cryptography could be a good replacement for old public key cryptographies that used before.

Table I is a comparison between key lengths between RSA with ECC. It shows the key length in elliptic-curve cryptography is very less that others like RSA [4]. In this table row indicates the length of keys with the same security level. For instance the security which can provide by the elliptic-curve cryptography (ECC) with 160 bits key size has the same security level when using the RSA with the 1024 key bits and so on. Therefore ECC easily can solve the problem of the key management by using less key length for more security.

Table 1. NIST Recommended Key Sizes

RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
1024	160
2048	224
3072	256
7680	384
15360	521

Another item NIST mentioned is about cost. Table II shows the ratio of computation costs between elliptic-curve cryptography and Diffie-Hellman for each key size also shows ECC has very less cost than others [7]. The cost of computation is combination of time, hardware and software. As the table shows that the cost of the computation will grows by expanding the key size in Diffie-Hellman cryptosystem, for example for key 80 bits the ratio of the cost of the Diffie-Hellman is three times more than the ECC algorithm and it is six times more in the case of 112 bits key length.

Table 2. Computation Costs

Relative Computation Costs of Diffie-Hellman and Elliptic Curves	
Security Level (bits)	**Ratio of DH Cost : EC Cost**
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

Another issue for cloud client is key generation. The speed of key generation also in ECC has better performance than RSA. As shown in figure 2, the test had done by windows operating system, Intel Celeron 1.86GHz processor [8]. In this figure the key sizes of ECC whit corresponding key size of RSA, have different computation time. By increasing the key size in RSA, the computation time will grow, but in ECC is almost same computation time. Therefore ECC has a better key generation time.

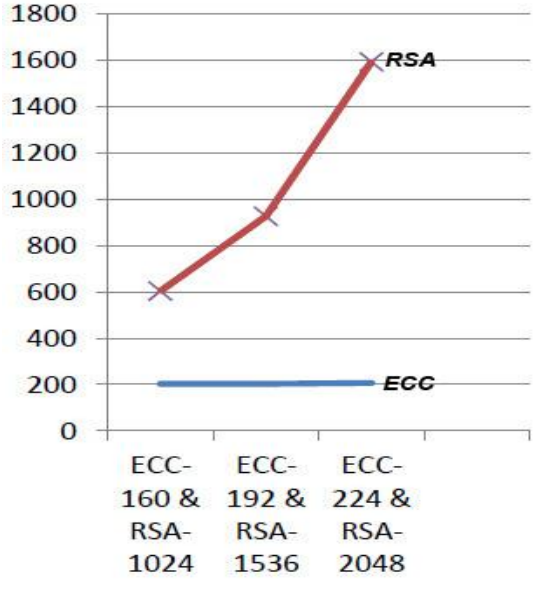

Figure 2: Key Generation (ms)

The elliptic-curve cryptography has fast encryption and decryption and specially decryption computation. The importance of decryption is about the cloud clients limitations which are very important in most of the cases. Using smart phones and tablets in these days is growing very fast and they have some limitation in processors and battery time. Other measurement is done by a machine with 1GB RAM and 1.6 GHz processor speed on Windows XP platform and the results are shown in Table III [9].

Table 3. CPU Time

p	A	b	CPU Time (Secs)	
			Encoding	Decoding
2011	9	7	0.01	0.000001
4093	9	7	1.11	0.000003
8191	10	17	0.85	0.000003
16381	1	17	3.7	0.000002
65521	7	29	0.7	0.000004

Three columns of this table indicate the initial parameters of the ECC algorithm shows ECC has a faster operation caparison with the RSA algorithm. Because of the nature of the elliptic-curve different initial parameters have different performance. The Standards for Efficient Cryptography Group (SECG) in the second version [10] proposed higher performance initial parameters for ECC with different key size. It helps the enterprise application implementer to select better parameters.

3. Inter-vm communication in cloud

The important concept in a cloud computing technology is the virtualization technology. Virtualization technology is used to achieve with the cloud computing technology. The cloud vendors usually use cryptography in communication channels and data storage area, but encrypted data is used below of the hypervisor layer which is responsible for the communication between the VMs in a cloud environment as shown in figure 3.

Cloud based application has an important role in new cloud based IT industries, for instance different enterprise organizations which are using the one of the services of cloud computing like PaaS or IaaS, which is obviously will use a different VM or even sometimes one organization use two different VM using two different virtual operating systems like windows and Linux operating systems, needs to exchange the secret information and pass messages between them through that environment. Hence, they need to use the robust security cryptosystems for their communication.

Because of the entity of the VM's in a cloud environment [1], you cannot be sure the neighbors VM is the good neighbor or it is the nosy VM that trying to sniff your information which you VM want to send to other VM's.

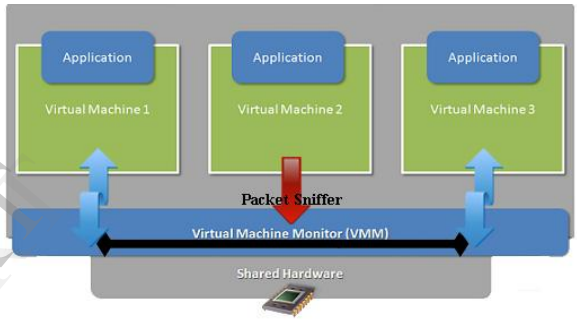

Figure 3: Model of Communication between VM's

The thing happening here is if one VM want to send a message to another VM, it uses IP which assigned to it from pool of network IP's, the message will capsulate with specified IP and sends to another VM. One of the major problems in this process is secure communication between two VM's which is nobody can ensure that there are no sniffers there or not [11]. So the only way we can overcome on this problem is use conversation language which no one can understand it except the sender and receiver and that is called as cryptography.

With these comparisons we can say that elliptic-curve cryptography is the better choice for the cloud environment and global applications.

4. Elliptic-Curve

An elliptic-curve is set of related points which create the curve with the standard equation in the form of $y^2 = x^3 + ax + b$, it must have no repeated root that satisfies the equation $4a^3 + 27b^2 \neq 0$ which create non-singular curve [12].

Figure 4 represents an elliptic curve with the parameters a, b defines as a = -1 and b = 0.

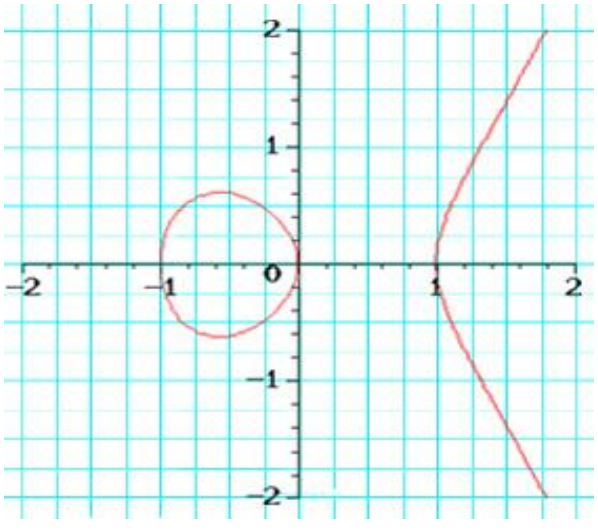

Figure 4: Elliptic-Curve of $y^2 = x^3 - x$

As we are shown in figure 4, an elliptic curve is completely differs from the ellipse curve.

The most important characteristic of the elliptic-curve are, it basically creates the Abelian group [5,10] of points and it is symmetric about the x-axis. It means suppose P_1 and P_2 are two points of the curve, then $P_1 + P_2 = P_2 + P_1$ for all points $P_1, P_2 \epsilon E(F_p)$ [5].

5. Elliptic-Curve Cryptography (ECC)

In 1985, Neal Koblitz [13] and Victor Miller [14] independently suggested designing new public-key cryptography based on the elliptic-curves. In late of 90's, this method standardized by some organizations which compromise it for commercial uses.

Elliptic curve cryptography (ECC) [5] is an asymmetric public-key cryptosystem like RSA public-key based on the elliptic curve related points calculation which level of security of ECC is depends on the difficulty of solving Discrete Logarithm Problem (DLP) [15,16]. The power of the security level of the ECC convinced everyone that it could be the one of the best replacements for the conventional public-key cryptographies. The major operations are "point addition" and "point multiplication" which point addition is used for finding a third point on the elliptic-curve. Point multiplication [17] calculates by repeating the addition operation. The major operation for elliptic-curve calculation is point multiplication. Elliptic-curve are mostly used over two finite fields. The prime field F_p , where p is a prime number [18,19], and the binary field F_2^m [20], where m is a positive integer [12].

In this article we are using prime field F_p for calculation of the elliptic-curves. All the operations based on the modular arithmetic by involving a prime number [21,12].

6. How ECC works

The overall calculation of elliptic-curve cryptography is based on calculating points of the selected elliptic-curve. First, we should select a, b parameters to able to define selected elliptic-curve by using standard formula $y^2 = x^3 + ax + b$.

Next, we calculate the some major points on the elliptic-curve and from now on we call it as a base - point. These points are the starting points of each part of curve that we use one of them to calculate other related points.

In elliptic-curve cryptography, we do not use the real number for each message; we assign the point to each part of plain text and create the term of plain points. Here instead of using plain text, we use plain point to calculate the cipher message. By using encryption operation we calculate cipher points and our message completely secure for passing it through the network. By the reverse operation we can decrypt cipher point to the plain point and then converting plain point to the plain text.

7. Conclusion

Because of the nature of the cloud computing environment especially multi tenancy of the cloud model, there are different user of virtual machines could be there. We cannot find out our neighbour is one the hackers which try to sniff our information or not. The best way to send our messages through the cloud environment are secure our messages provides by strong and robust cryptographic algorithm like ECC. One of the advantages is each user can be using different curve formula [11].

Maybe one of the disadvantages of ECC is the complexity of the algorithm, but in such an environment which we cannot define the abilities of our enemies we need such a complexity, otherwise what is the importance of the cryptography.

On the other hand the size of the key of this cryptosystem gives us this ability to use it in a totally distributed environment with different devices from small size with limited computing abilities to big size

devices with strong ability of computation. In this case key management is easier.

And another thing which is very important for distributed environment is the decryption operation is very fast [9] at the receiving participant.

REFERENCES

[1] C. S. Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0", Cloud Security Alliance, 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A View of Cloud Computing, Communications of the ACM", Vol. 53, No. 4, p 50-58, April 2010.

[3] W. Stallings, "Cryptography and Network Security Principles and Practice", 4th ed., Prentice Hall, New Jersey, 16 November 2005.

[4] V. Gupta, S. Gupta, S. Chang, and D. Stebila, "Performance analysis of elliptic curve cryptography for SSL," in Proc. ACM Wkshp. Wireless Security, Sept. 2002.

[5] SECO Staff, "SEC 1: Elliptic Curve Cryptography, Version 1.0", Standards for Efficient Cryptography Organization, September 2000.

[6] M. Höfer, G. Howanitz, "The Client Side of Cloud Computing", University of Strausburg, 1-20, 1 July 2009.

[7] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, "High-Performance Scalar Mul-tiplication using 8-imensional GLV/GLS Decomposition", In G. Bertoni and J.-S. Coron, Cryptographic Hardware and Embedded Systems – CHES 2013. Lecture Notes in Comput. Sci.8086, 2013.

[8] A. Tripathi, P. Yadav, "Enhancing Security of Cloud Computing using Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887), Vol. 57, No.1, November 2012.

[9] P. Bh, D.Chandravathi , P.Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method" , (IJCSE) International Journal on Computer Science and Engineering, Vol.02, No.05, 2010.

[10] H. Kamarulhaili, L.K. Jie, "Elliptic Curve Cryptography and Point Counting Algorithms", School of Mathematical Sciences, Universiti Sains Malaysia, Minden, Penang, Malaysia.

[11] A.J. Menezes, S.A. Vanstone, "Elliptic curve cryptosystems and their implementation", J. Cryptology, Vol 6, 13 August 1992.

[12] M.O. Rabin, "Probabilistic algorithm for testing primality", J. of Number Theory, Vol. 12, No. 1 , 1980, p 128–138.

[13] N. Koblitz, "Elliptic curve cryptosystems. Mathematics of Computation", 48:203–209,1987.

[14] V. Miller, "Use of elliptic curves in cryptography", in Advances in Cryptology—CRYPTO '85, Lecture Note in Computer Science, Vol. 218, New York: Springer-Verlag, 1986.

[15] K. Araki, T. Satoh, S. Miura, "Overview of Elliptic Curve Cryptography", Lecture Notes in Computer Science Vol. 1431, 1998.

[16] Z. Cheng, "Simple Tutorial on Elliptic Curve Cryptography", School of Computing Science, December 2004.

[17] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields," Lecture Notes in Computer Science , Vol. 1965, 2001.

[18] M. Brown, D. Hankerson, J. Lopez, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields", In CT-RSA, p. 250–265, London, UK. Springer-Verlag, 2001.

[19] F. Morain, "Building cyclic elliptic curves modulo large primes", In Advances in Cryptology – Eurocrypt'1991 , volume 547 of Lecture Notes in Computer Science , Springer-Verlag, 1991.

[20] J. Lopez, R. Dahab, "An Overview of Elliptic Curve Cryptography", Technical report, State University of Campinas, Brazil, May 2000.

[21] G.L. Miller, "Riemann's hypothesis and tests for primality", Proc. Seventh Annual ACM Symp. on the Theory of Comptng. Albuquerque, New Mex., May 1975, pp. 234–239; extended vers. available as Res. Rep. CS-75-27, Dept. of Comptr. Sci., U. of Waterloo, Waterloo, Ont., Canada, Oct. 1975.