International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

A Comparison of ECC and Improved ECC Algorithm for Cloud Security

V. Vincy*[1], Dr. B. Sathees Kumar[2]

[1]MPhil Research Scholar, Department of Computer Science, Bishop Heber College (Autonomous), Trichy, Tamil Nadu, India

[2]Associate Professor Department of Computer Science, Bishop Heber College (Autonomous), Trichy, Tamil Nadu, India

ABSTRACT

Cloud computing is a distributed environment that encompasses thousands of computers that work in parallel to perform a task in lesser time than the traditional computing models. This parallelism enables the low cost virtualization of hardware resources with increased computational performances. Cloud computing provides tremendous opportunity for small and medium scale enterprises to grow their business using IT services with zero deployment cost. Whenever, a task is distributed over web, there encounters a series of potential threats that challenges the security of data such as buffer overflow, session hijacking and black hole attacks. A cloud computing based services also face such kinds of security issues where applications deployed on cloud can face same kind of attacks as that on client-server model. Storage as a Service (SaaS) based applications are vulnerable to virus attacks .Online operating systems are available on cloud to the user for free .Viruses can spread as attachments of email, of part of the software or can stay in Master Boot Record (MBR) of the operating system available on cloud. Worms residing on one system in cloud can migrate to another system on its own. Trojan horse is software with wrong intentions. Thus the present system needs an effective mechanism to address the problem encountered in cloud computing.This thesis is intended to provide an enhanced security service in cloud computing model using an enhanced Elliptic Curve Cryptography algorithm for securing user data over cloud. The thesis is also extended to present both the theoretical and empirical results of the proposed improved elliptic curve based public key cryptography to prove that the model is better than the traditional RSA based schemes in terms of encryption, decryption time and key sizes.

Keywords: Cloud Computing, ECC, AES

I. INTRODUCTION

Cloud computing is a flexible, cost-effective and established delivery platform for providing business or consumer IT services over the Internet. Cloud computing chains distributed service oriented architecture, multi-users and multi-domain administrative communications; it is more level to security threats and vulnerabilities. At present, a main concern in cloud acceptance is its security and Privacy. Intrusion prospects within cloud environment are several and with high gains. Security and Privacy issues are of more concern to cloud service providers who are essentially hosting the services. In most cases, the provider must assurance that their infrastructure is secure and clients' data and applications are secure by implementing security policies and mechanisms. While the cloud customer must guarantee that provider have full proper security measures to keep their information.

The issues are organized into several common categories: trust, architecture, identity management, software isolation, data protection, availability Reliability, Ownership, Data Backup, Data Portability and Conversion, Multiplatform Support and Intellectual Property. A cloud computing based services also face such kinds of security issues where applications deployed on cloud can face same kind of attacks as that on client-server model. Storage as a Service (SaaS) based applications are vulnerable to virus attacks This thesis is intended to provide an enhanced security service in cloud computing model using an enhanced Elliptic Curve Cryptography algorithm for securing user data over cloud.

The thesis is also extended to present both the theoretical and empirical results of the proposed improved elliptic curve based public key cryptography to prove that the model is better than the traditional AES based schemes in terms of encryption, decryption time and key sizes.

II. RELATED WORK

Arora et al. [2017] presented a Hybrid Cryptographic System (HCS) that combines the benefits of both symmetric and asymmetric encryption thus resulting in a secure Cloud environment.

Thu Yein Win et al. [2017] proposed a novel big data based security analytics approach to detecting advanced attacks in virtualized infrastructures. Network logs as well as user application logs collected periodically from the guest virtual machines (VMs) are stored in the Hadoop Distributed File System (HDFS).

Xiao-tao et al. [2016] to introduced the reference model, cloud computing security established cloud security content matrix, cloud application system framework is constructed.

Services in cloud computing platform is scalable, it can be a specific server fann, can also be another platform, a general cloud computing platform generally includes storage equipment, network equipment, computing equipment, security equipment, platform can provide a variety of service form, such as software as a service, the data as a service, platform as a service and infrastructure as a service, communication as a service etc.

But in a complex system of Internet of things application of cloud computing technology, information security of cloud computing is very important, in the application process, should grasp the principle of easy to operation and maintenance and so on, fully considering the reliability, availability, confidentiality, integrity and no repudiation basic properties, such as security cloud system framework.Jayapandian et al. [2016] provided the foremost goal of schemed any encryption algorithm is to fleece the original note and send the non readable text message to the receiver so that secret message communication can take place done.
The web.Ahmad et al. [2017] discusses the security issues of the cloud computing. Further the paper illustrates upon the security solutions for the virtualization and web services, two major enabling technologies of cloud computing.Shokri et al. [2016] to develop a novel epidemic model to capture the, possibly time-dependent, dynamics of information propagation among users. Used in the Bayesian inference framework, this model helps analyze the effects of various parameters, such as users' querying rates and the lifetime of context information, on users' location privacy. Chhabra et al. [2016] the proposed methodology balances the load of whole data into chunks so that parallel processing will increase and execution time will decrease.

This helps to avoid alterations in the original data while allocating the data objects. If the guilty agent (GA) is recognized, he or she can be put on the hit

list and can debarred from being a part of our company or industry. In previous times, watermarking technique is used widely for detecting the unauthorized agents.

Bhamare et al. [2016] work, they use the UNSW dataset to train the supervised machine learning models. They then test these models with ISOT dataset. They present to results and argue that more research in the field of machine learning is still required for its applicability to the cloud security.

Yuan et al. [2016] paper, they study an automatic testing system for public cloud on data security risks. To this end, they first establish a framework based on SOA (Service Oriented Architecture), which provides a capability to precede data security tests on cloud automatically. Second, based on the framework, they implement a cloud security testing system, which includes data confidentiality test and data deletion risk test.

El Makkaoui et al. [2016] to provided a new cloud security and privacy model (CSPM) into layers which can be taken into account by cloud providers during all the stages of cloud services building and monitoring.

III. ECC ALGORITHM FOR ENHANCING CLOUD

In this research work AES algorithm is implemented for authentication purpose and Improved ECC algorithm is used for file (document) encryption in Cloud storage. There is facility to block unauthorized user, forget password and secret no. is sent to personal email account along with file encryption, upload, download and decryption. First objective of proposed work is to make the system secure so that only authorized user can login in the cloud, if any unauthorized user try to access our private cloud here can easily track and permanently block his/her IP and even MAC address of device from where he/she is try to access our private cloud. Second is to make the file sharing in private cloud totally secure using ECC algorithm, and which is hard to decrypt and to make the packets travel securely in network using ECC, so that any hacker cannot intercept or decrypt any packet.

Figure 1 shows the complete working for proposed system. It describes that after registration if any user is trying to login and if password is wrong or MAC address is wrong for 5 times the account was blocked. Figure 2 describes the possible operations for proposed system; these operations can be applied on document (files) for their security.

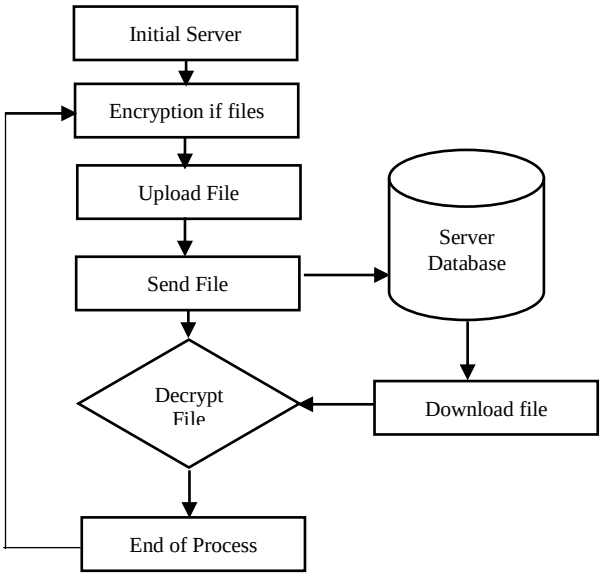

Figure 1. The flowchart for file process.

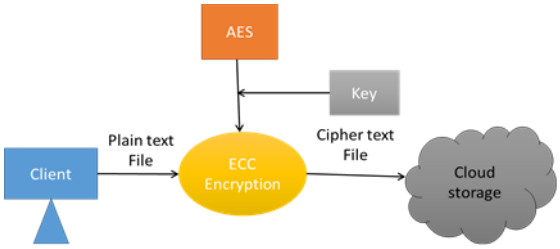

Figure 2. Proposed Architecture

IV. ELLIPTIC CURVES

First of all: what is an elliptic curve? Wolfram MathWorld gives an excellent and complete definition. But for our aims, an elliptic curve will simply be the set of points described by the equation:

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

Where $4a^3+27b^2\neq0$ (this is required to exclude singular curves). The equation above is what is called *Weierstrass normal form* for elliptic curves.

A.Encryption

Let "m" be the message that we are sending.
Here 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 C1 and C2.
C1 = k * p
C2 = M + k * Q

B. Decryption

The message "M" that was sent is written as following equation,
M = C2 - d * C1

V. ADVANCEDENCRYPTION STANDARD (AES)

The Advanced Encryption Standard (AES), also known as Rijndaelo is a design for the encryption of electronic data recognized by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is based on the ijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a suggestion to NIST during the AES selection procedure. Rijndael is a family of ciphers with different key and block sizes.

For AES, NIST select three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been accepted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm explains by AES is a symmetric-key algorithm, meaning the similar key is used for both encrypting and decrypting the data.

VI. ECC with AES

This section contains the working with elliptic curves which are defined over Zp. These are often called the prime curves and can be far simpler to work with as here can reduce modulo p at each stage. Suppose we have an elliptic curve, E, over Zp. In this case we have a cubic equation in which the variables and coefficients take values on the set of integers 0, 1, ... (p – 1) and all calculations are performed modulo p. y 2 ≡ x 3 - Ax - B (mod p) here write Ep(A, B) for the set of integers (x, y) that satisfy the above equation, together with a point at infinity, ∞.

The set E11(1, 6) is the set of integers (x, y) that satisfy
y 2 ≡ x 3 - x - 6 (mod 11)
Here can see that (x, y) = (7, 9) is in this set as
9 2 (mod 11) = (73 + 7 + 6) (mod 11)
81 (mod 11) = 356 (mod 11) ⇐⇒ 4 = 4

To find all the points in E11 (1, 6) here find all the possible values x 3 + x + 6 (mod p) and then see what values of y 2 will match. There are 11 choices of x, the integers {0, 1... 10}. Subbing these values in turn into the cubic and reducing modulo 11 will give us the possible values of y 2:

x = 0 =⇒ RHS = 6 x = 6 =⇒ RHS = 228 ≡ 8
x = 1 =⇒ RHS = 8 x = 7 =⇒ RHS = 356 ≡ 4
x = 2 =⇒ RHS = 16 ≡ 5 x = 8 =⇒ RHS = 526 ≡ 9
x = 3 =⇒ RHS = 36 ≡ 3 x = 9 =⇒ RHS = 744 ≡ 7

$x = 4 \Longrightarrow RHS = 74 \equiv 8$ $x = 10 \Longrightarrow RHS = 1016 \equiv 4$
$x = 5 \Longrightarrow RHS = 136 \equiv 4$

So we can see that the possible values of y 2 are {3, 4, 5, 6, 7, 8, 9} i.e. y^2 cannot be 0,1,2 or 10. Next examine the 10 possible values of y and identify which values of x they could be paired with to give a point on the curve.

$y = 0 \Rightarrow y^2 = 0 \Rightarrow$ No Points $y = 6 \Rightarrow y^2 = 36 \equiv 3 \Rightarrow x = 3$
$y = 1 \Rightarrow y^2 = 1 \Rightarrow$ No Points $y = 7 \Rightarrow y^2 = 49 \equiv 5 \Rightarrow x = 2$
$y = 2 \Rightarrow y^2 = 4 \Rightarrow x = 5, 7, 10$
$y = 8 \Rightarrow y^2 = 64 \equiv 9 \Rightarrow x = 8$
$y = 3 \Rightarrow y^2 = 9 \Rightarrow x = 8$ $y = 9 \Rightarrow y^2 = 81 \equiv 4 \Rightarrow x = 5, 7, 10$
$y = 4 \Rightarrow y^2 = 16 \equiv 5 \Rightarrow x = 2$ $y = 10 \Rightarrow y^2 = 100 \equiv 1 \Rightarrow$ No Points
$y = 5 \Rightarrow y_2 = 25 \equiv 3 \Rightarrow x = 3$

E11(1, 6) = {(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9), ∞} An m-file, PC.m, to find and plot all the points on a prime curve was constructed and is stored in Appendix C.2. This m-file takes as its inputs, A, B and p and produces two vectors X, Y which contain all the points (x, y) that lie on $y\ 2 \equiv x\ 3 + Ax + B \pmod p$. When run on this example it verified that we had found all the points in E11(1, 6) and plotted the graph below. Here can see that the points are symmetric about the line y = 5.5

Here can perform the elliptic curve addition operation on prime curves; however we reduce modulo p at each step. For example, still considering E11 (1, 6)

If P = (8, 3) then we know that –P = (8, –3). Working modulo 11 we see that –P = (8, 8) which is also a point in E11(1, 6).
Let P = (8, 3) and Q = (3, 5). Then to find R = P + Q:
$m = (5 – 3) /(3 – 8) = 2/ –5 \equiv 2 /6 = 1 /3 = 1 \times 4 = 4$

The penultimate step involved taking the multiplicative inverse of 3 in Z11. Now proceed to show that

$x_R = 4^2 – 8 – 3 = 5$, $yR = 4(8 – 5) – 3 = 9$ So in E11(1, 6) we find (8, 3) + (3, 5) = (5, 9). • Again let P = (8, 3). To calculate 2P = P + P:
$m = (3(8^2) + 1) / (2 * 3) = 193 /6 \equiv 6/ 6 = 1 \pmod{11}$
Then $x_2P = 1^2 – 2(8) = –15 \equiv 7 \pmod{11}$
$y_2P = 1(8 – 7) – 3 = –2 \equiv 9 \pmod{11}$
So in E11 (1, 6) we find 2(8, 3) = (7, 9).

The earlier m-file for performing elliptic curve addition was modified for use with prime curves. It now reduces modulo p at each stage using mod function and find the inverse of elements so the final answer is an element on a prime curve. It contains the same inputs and outputs as m but the user must input p in addition. It makes use of the m-file inseam which is stored in Appendix C.4. This m-file takes as its inputs a number N and a prime p and outputs the inverse of N in the group Z_p. The m-file m was used to calculate the remaining entries in the addition table overleaf (Table 2.1). In show that (2, 7) is a generator of this group and so it is isomorphic to Z_{13}.

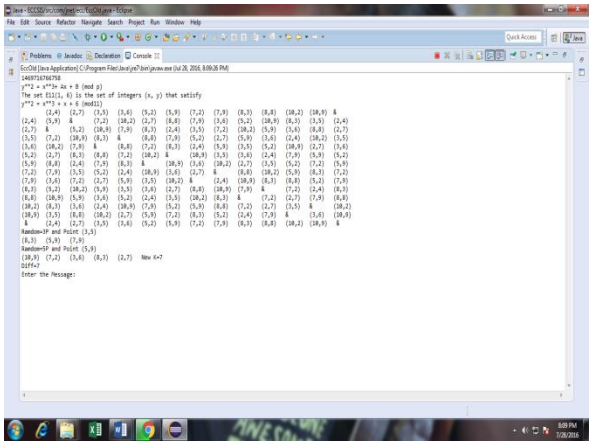

Figure 3. Key Generation output point

A Cloud service is a platform to build networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A cloud service consists of a representation of each user (often a profile), his/her

social links, and a variety of additional services. Most cloud services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered.

A.KeyComparision for Standard ECC and Improved ECC Algorithm

Figure 4 represents the Key comparison Time chart of the resources with respect to expected completion time of tasks.

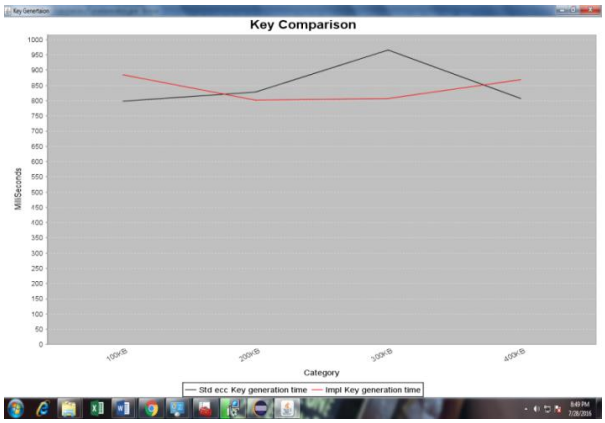

Figure 4. Key Comparison

B.Encryption Time Comparision for Stadard ECC and Improved ECC Algorithm

Figure 5 represents the Encryption Time chart of the resources with respect to expected completion time of tasks.

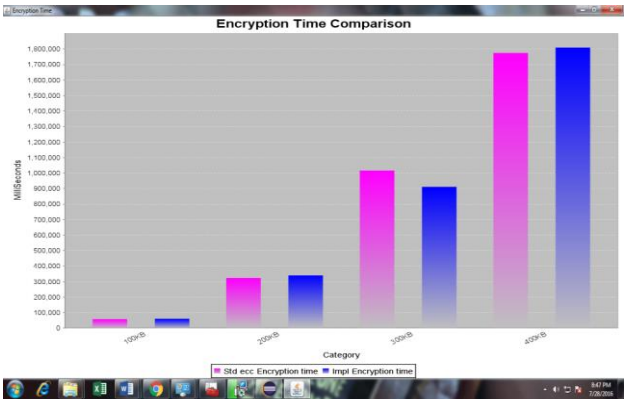

Figure 5. Encryption Time

C.DecryptionTime Comparision for Standard ECC and Improved ECC Algorithm

Figure 6 represents the Decryption Encryption Time chart of the resources with respect to expected completion time of tasks.

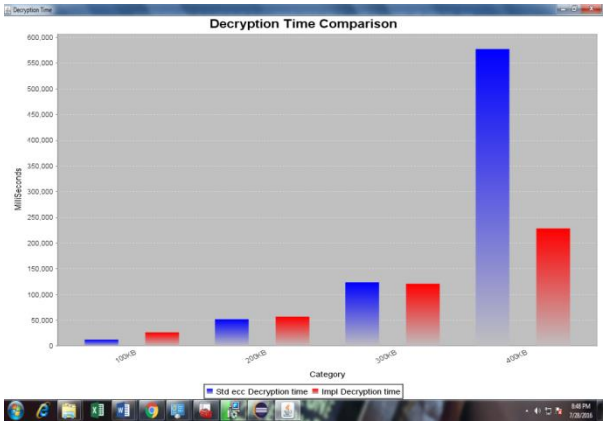

Figure 6. Decryption Time

D. Summary

This section contains the working with elliptic curves which are defined over Zp. These are often called the prime curves and can be far simpler to work with as here can reduce modulo p at each stage.

VII. CONCLUSION AND FUTURE ENHANCEMENT

Conclusion

Data has become more important as the methods which are used to ensure security not only need to be strong and efficient but should be easy to implement and execute. Cloud computing is a modern concept that not just speeds up computing and cut costs. However, several challenges still weigh down the technology. Resolving security problems with cloud computing is one such major challenge. It requires an adequate understanding of both the security issues in cloud computing implementation as well as the solutions presently available to address these. The security model is used to improve security without degrading the performance of the system. Main goal of future improvement is providing more security by using more secure algorithm whose security can't be broken.

Simulation results shows that AES algorithm is best for authentication and ECC algorithm used for security has better performance than other techniques. Since ECC has not any known security weak points till now, it can be considered as an excellent standard encryption algorithm. The experimental results reveal that the proposed method offers better performance over previous work.

Future Enhancement

In future here can use ECC algorithm for securing audio and video data. Because, In the area of security, research area of speech is very wide. The Android platform of Smartphone's is a powerful platform and is used in 80% of Smartphone's today. The sensors that come with the mobile devices further give a context to cloud applications and opens up a new set of possibilities.

VIII. REFERENCES

[1]. Arora, Akshay, Abhirup Khanna, Anmol Rastogi, and Amit Agarwal. "Cloud security ecosystem for data security and privacy." In Cloud Computing, Data Science & Engineering-Confluence, 2017 7th International Conference on, pp. 288-292. IEEE, 2017.

[2]. Thu Yein Win "Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing". IEEE Transactions on Big Data (Volume: PP, Issue: 99 2017.

[3]. Xiao-tao, Xu, Chen Zhe, Jiang Fei, and Wang Hui-tao. "Research on service-oriented cloud computing information security mechanism." In Computer and Communications (ICCC, 2016 2nd IEEE International Conference on, pp. 2697-2701. IEEE, 2016.

[4]. Jayapandian, N., AMJ Md Zubair Rahman, R. B. Sangavee, and R. Divya. "Improved cloud security trust on client side data encryption using HASBE and Blowfish." In Green Engineering and Technologies (IC-GET, 2016 Online International Conference on, pp. 1-6. IEEE, 2016.

[5]. Ahmad, Naim. "Cloud computing: Technology, security issues and solutions." In Anti-Cyber Crimes (ICACC, 2017 2nd International Conference on, pp. 30-35. IEEE, 2017.

[6]. Shokri, Reza, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and Jean-pierre Hubaux. "Hiding in the Mobile Crowd: Location Privacy through Collaboration." In IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, SPECIAL ISSUE ON "SECURITY AND PRIVACY IN MOBILE PLATFORMS. 2016.

[7]. Chhabra, Sakshi, and Ashutosh Kumar Singh. "Dynamic data leakage detection model based approach for MapReduce computational security in cloud." In Eco-friendly Computing and Communication Systems (ICECCS, 2016 Fifth International Conference on, pp. 13-19. IEEE, 2016.

[8]. Bhamare, Deval, Tara Salman, Mohammed Samaka, Aiman Erbad, and Raj Jain. "Feasibility of Supervised Machine Learning for Cloud Security." In Information Science and Security (ICISS, 2016 International Conference on, pp. 1-5. IEEE, 2016.

[9]. Yuan, Man, Shuning Pang, and Qiang Gao. "Design and development of data security automatic testing system on public cloud." In Software Engineering and Service Science (ICSESS, 2016 7th IEEE International Conference on, pp. 992-995. IEEE, 2016.

[10]. El Makkaoui, Khalid, Abdellah Ezzati, Abderrahim Beni-Hssane, and Cina Motamed. "Cloud security and privacy model for providing secure cloud services." In Cloud Computing Technologies and Applications (CloudTech, 2016 2nd International Conference on, pp. 81-86. IEEE, 2016.