ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

ECC Algorithm & Security in Cloud

[I]C. Nithiya, [II]R. Sridevi
[I]M. Phil. Scholar, Dept. of Computer Science, PSG College of Arts and Science, Coimbatore, India.
[II]Assistant Professor, Dept. of Computer Science, PSG College of Arts and Science, Coimbatore, India.

Abstract
Security in cloud computing is an evolving area in today's world. It is subject of concern for Cloud Technology Services. One of the measures which customers can take care of is to encrypt their data before it is stored on the cloud. This work is intended towards providing security service such as confidentiality in the cloud services which use Elliptic Curve Cryptography (ECC) algorithm instead of familiar and generalized RSA for data encryption because of its advantages in terms of smaller key sizes, lower CPU time and less memory usage.

Keywords
Security, Elliptic Curve Cryptography, RSA, Key Generation and Cloud Technology.

I. Introduction

With the invention of cloud, the days of keeping all your documents, photos, music files etc. on your computer's hardware are gradually coming to a close. Today, the cloud storage is fulfilling the need for more storage space to hold all of your digital data. Cloud storage providers operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. As shown in Fig. 1, cloud storage can be used from smaller computing devices to desktop computers and servers.

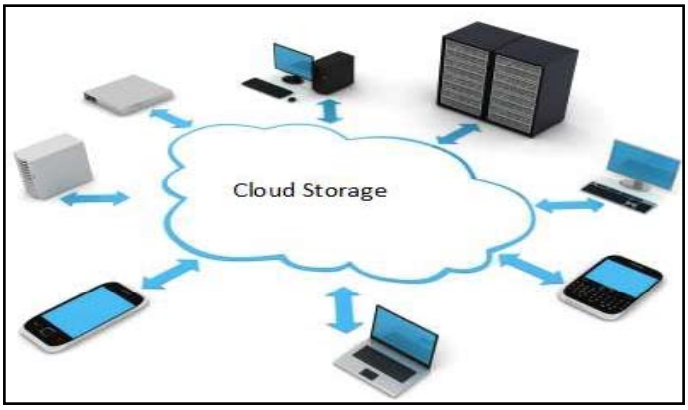

Fig. 1 : Cloud storage

Cloud computing enhances the distribution of services for the Internet users. It is a computing mission on resource pools that include a large amount of computing resources. With cloud computing advancement as a new resource of computing on the Internet that provide assorted kinds of cloud services, also bring some security problems on the distribution of services over the Internet. At the moment, most computing systems provide digital identity for the users to access their services; these bring some inconveniences for hybrid cloud that includes multiple private and public clouds. However, the advantage of using cloud are numerous which include: i) reduced hardware and maintenance cost; ii) accessibility around the globe, iii) flexibility and the highly automated process wherein customer need not worry about software up-grading, physical hardware purchases and some basic infrastructures which tend to be a daily problem in computing environments. The Cloud Computing systems that provide services to the Internet users apply the asymmetric or public key and private or traditional identity based cryptography that has some identity elements that fit well in the requirement of cloud computing. This work aims at improving cloud computing within Cloud Organizations with encryption awareness based on Elliptic Curve Cryptography.

To secure data, most systems use a combination of techniques, including:

1. Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a user needs an encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.
2. Authentication processes, which require creating a user name and password.
3. Authorization practices -- the client lists the people who are authorized to access information stored on the cloud system.

Many corporations have multiple levels of authorization. For example, a front-line employee might have very limited access to data stored on a cloud system, while the head of human resources might have extensive access to files. Cloud storage approach poses a potential security threat to your data and moreover, only the password access to storage is not sufficient as the password can be hacked by an intruder. Also the data can be captured en-route to the storage services. The need to access cloud storage on thin clients and mobile devices is becoming an emerging application. But due to smaller processor speed and run time memory; these devices need an algorithm which can be used in such small computing devices. Security of stored data and data in transit may be a concern when storing sensitive data at a cloud storage provider.

II. ECC Algorithm

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security

products. RSA has been developing its own version of ECC. The properties and functions of elliptic curves have been studied in mathematics for 150 years. Their use within cryptography was first proposed in 1985, (separately) by Neal Koblitz from the University of Washington, and Victor Miller at IBM. An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

A. Computation of Point on the Curve

The security of ECC algorithm depends on its ability to compute a new point on the curve given the product points and encrypt this point as information to be exchanged between the end users.

B. Choice of Field

Although RSA public key cryptosystem is a secure asymmetric-key cryptosystem, its security comes with a price of larger key sizes and computational power. Many researchers have looked for an alternative to this system with a smaller key size while maintaining the same level of security. The ECC system is based on the concepts of Elliptic Curves. To analyze the time taken by an algorithm researches have introduced polynomial time algorithms and exponential time algorithms. Algorithms with smaller computation can be evaluated with polynomial time algorithms and complex computations can be evaluated with exponential time algorithms. The equation of an elliptic curve is given as,

$y2 = x3 + ax + b$

C. Key Generation

Key generation is an important part where an algorithm should generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, select a number, d within the range of n. Generate the public key using the following equation,

$Q = d * P$

Where d = the random number selected within the range of (1to n-1). P is the point on the curve, Q is the public key and d is the private key.

D. Encryption

Let 'm' be the message that has to be sent. Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 -(n-1)]. Two cipher texts will be generated let it be C1 and C2.

$C1 = k * P$

$C2 = M + (k * P)$

E. Decryption

Use the following equation to get back the original message 'm' that was sent.

$M = C2 - d * C1$

M is the original message that was sent.

III. Advantages of ECC over RSA

1. Shorter keys are as strong as long key for RSA.
2. Low on CPU consumption.
3. Low on memory usage.
4. Size of encrypted data is smaller.

In today's world ECC algorithm is used in case of key exchanges by certificate authority (CA) to share the public key certificates with end users. Elliptic Curve Cryptography is a secure and more efficient encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA. For e. g. a 256-bit ECC public key provides comparable security to a 3072-bit RSA public key. The aim of this work is providing an insight into the use of ECC algorithm for data encryption before uploading the documents on to the cloud. Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths. Every participant in the public key cryptography will have a pair of keys, a public key and private key, used for encryption and decryption operations. Public key is distributed to all the participants where as private key is known to a particular participant only.

IV. Simulation

A. System Configuration

The System configuration used in the experiments is a Windows 7 operating system with 4 GB RAM and 2. 6 GHz processor.

B. Assumptions

i) Block Size: The block sizes are assumed to be as follows which are the actual block sizes to be used for RSA. The same block sizes are used for both ECC and RSA which is based on the key size.
Encryption Block Size: ((keySize / 8) - 11)
Decryption Block Size: (keySize / 8)
ii) Key Size: As per The National Institute of Standards and Technology (NIST) Guidelines for Public-Key Cryptography, the ECC and RSA comparable key sizes with equivalent Security Levels are shown in Table 1.

Table 1: Key sizes with equivalent security levels

ECC	RSA
160	1024
224	2048
256	3072
384	7680
512	15360

iii) Parameters: To compare the performance characteristics of the RSA and ECC encryption algorithms, the parameters used for simulation are:

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

• Key Generation Time
• Encryption Time
• Decryption Time

Because of the timing mismatch in each of these 3 parameters simulation performed repetitive tests for each parameter for about 20 times to get the average timings of the parameters.

V. Results

Table 2 provides the key generation, as well as encryption and decryption times for ECC and RSA.

Table 2: Test Results

File size (KB)	Key Size (bits)	ECC Algorithm				RSA Algorithm			
		Key Gen Time (ms)	En-crypt Time (ms)	Decrypt Time (ms)	Size of En-crypt-ed File (KB)	Key Gen Time (ms)	En-crypt Time (ms)	De-crypt Time (ms)	Size of En-crypted File (KB)
6534	160	252	2374	1381	6534				
6534	224	262	943	1033	6534				
6534	256	270	1039	964	6534				
6534	384	282	772	755	6534				
6534	512	312	698	687	6534	654	14031	111019	7890
6534	1024					872	18190	300529	7148
6534	2048					1996	29970	998038	6827
6534	3072					16692	41872	210353	6727

VI. Analysis of Test Results

A. Key Generation Time

In both systems the key generation times were not the same every time, even though the key length is the same and it can sometime a take very long time to generate the keys. Figure 2 shows that for smaller key sizes the key generation time is almost equal in both cases, but as the key size grows RSA takes more amount of time to generate the keys and this time increases exponentially by the key size.

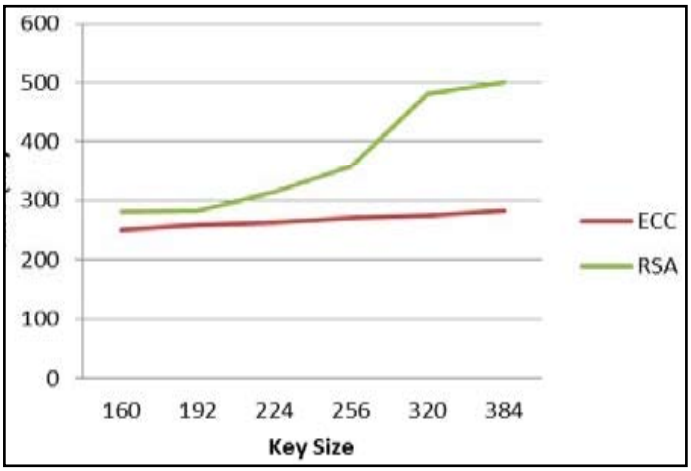

Fig. 2: Comparison of Key Generation Time for RSA and ECC

B. Encryption/Decryption Time

Figure 3 shows the Encryption times for ECC and RSA algorithms. Since JAVA implementation of RSA doesn't support key sizes lesser than 512 bits length, simulation had to compare the encryption/ decryption times between these two algorithms with different key sizes. Looking at the results, for smaller key sizes ECC provides much faster encryption/ decryption as compared to RSA. Since RSA uses higher key sizes the encryption/decryption times grow exponentially with the given key size.

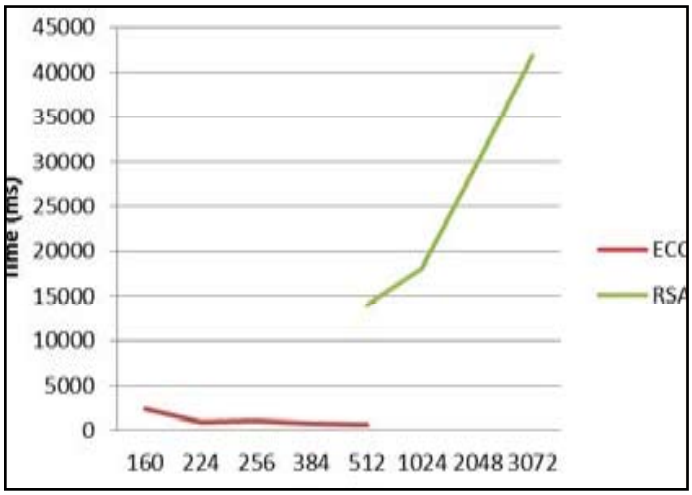

Fig. 3 : Comparison of Encryption times

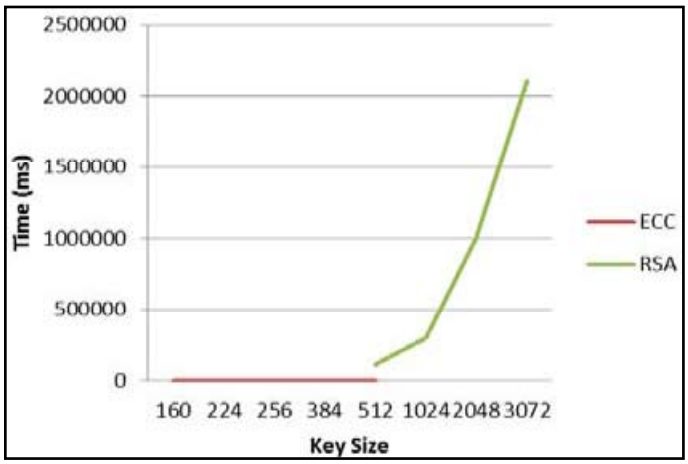

Fig. 4: Comparison of Decryption times

Figure 4 shows the decryption times. Time taken by two algorithms for encryption shows that; ECC is much faster than RSA. Based on the input key size ECC encryption time varies linearly whereas in case of RSA it increases exponentially due to the large amount of computation involved and it remains the exponential increase in decryption time too, as shown in the Figure 4. Even though the decryption time is lesser than the encryption time in both algorithms, the decryption time varies exponentially with key size for RSA and it remains linear for ECC as the case with encryption.

VII. Conclusion

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security. Although ECC's security has not been completely evaluated, it is expected to come into widespread use in various fields in the future. After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA. The ECC has many advantages due to its ability

to provide the same level of security as RSA yet using shorter keys. However, its disadvantage which may even hide its attractiveness is its lack of maturity, as mathematicians believed that enough research has not yet been done in ECC. The future of ECC looks brighter than RSA as today's applications (smart cards, pagers, and cellular telephones etc.) cannot afford the overheads introduced by RSA. At least, in today's small computing devices ECC can be used for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to RSA. Thus, ECC makes it an ideal choice for portable, mobile and low power applications and their integration with cloud services. This work compares the time taken by the two algorithms for key generation and encryption. The importance of this work is to use ECC algorithm in cloud storage which has better security services. This work can be extended to compare ECC with other algorithms used for digital signatures, key exchanges as well as to provide the data integrity.

VIII. Acknowledgement

I would like to give special thanks to my guide Mrs.R.Sridevi for giving me the chance to learn and understand the Cryptography concepts during my time in PSG College of Arts and Science. I would also like to thank my parents friends and brother for their continuous support.

References

[1] *Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_cryptograp hy*
[2] *RSA (algorithm), http://en.wikipedia.org/wiki/RSA_(algorithm)*
[3] *Chakraborty, T.K.; Dhami, A.; Bansal, P.; Singh, T. "Enhanced public auditability & secure data storage in cloud computing". 3rd IEEE International Advance Computing Conference (IACC), 2013.*
[4] *W.Diffie and M. Hellman." New Directions in Cryptography". IEEE transactions on Information Theory. IT-22(1978).472-492.*
[5] *William Stallings, "Cryptography and Network Security Principles and Practices", 4th edition, Pearson Education Inc, 2006.*

Authors Profile

C. Nithiya. She received her bachelor in Computer Technology in PSG College of Technology, Coimbatore in 2013. She did her master degree in Master of Computer Applications in PSG College of Arts and Science and continues her research in Information Security.

R. Sridevi. She is working as an Assistant Professor in Computer Science, PSG College of Arts and Science, Coimbatore. She finished her Post Graduate and MPhil under Bharathiar University, Coimbatore. She has currently submiteed her Phd thesis. Her area of specialization includes Network Security, Cryptography and Data mining.