International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing

Depavath Harinath

Lecturer, Department of Computer Science, Hyderabad, Telangana, India

Abstract: ***Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. This study aims to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats and the issues associated with cloud computing.***

Keywords: Cloud Computing, Cryptography, Network Security

1. Introduction

Cloud computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

2. Key Features of Cloud Computing

(A) The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":

1) *On-demand self-service:* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2) *Broad network access:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3) *Resource pooling:* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4) *Rapid elasticity:* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.
5) *Measured service:* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

(B) Types of Clouds

Depending on the access scope, cloud can be classified as *public cloud, private cloud, hybrid cloud and Community cloud.*

1) **Private Cloud:** Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.
2) **Public Cloud:** A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their data center and access is generally via the Internet.
3) **Hybrid Cloud:** Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity

needs that can not be met by the private cloud.

4) **Community cloud:** Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party, and either hosted internally or externally. Therefore Community cloud involves sharing infrastructure between organizations of same community like all government organizations within same sate.

(C) Based on the services provided cloud is classified as follows:

These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

1) ***Software as a Service (SaaS)*** where the providers offers various applications on a cloud infrastructure. Users can access software application hosted by cloud vendor through a thin client interface such as web browser. Like Salesforce.com offers online CRM space, Google‟s Gmail, Google docs, Microsoft‟s online version of office BPOS (Business Productivity Online Standard Suite).
2) ***Platform as a Service (PaaS)*** involves offering a development platform for customers on cloud where he can deploy his own applications without installing any platform or tools on their machines. Few PaaS providers are Google‟s Application Engine, Microsoft‟s Azure, etc.
3) ***Infrastructure as a Service (IaaS)*** involves offering hardware recourses like storage, network and other fundamental computing resources where the customer is able to deploy and run arbitrary software, which can include OS and applications. IaaS are provided by Amazon Ec2, Amazon S3, Rackspace Cloud Servers etc.

In spite of advantages of cloud computing, trusting the system is more important as the real asset of any organization is the data which is available on cloud. This trust depends on the data security and privacy issues. The meaning of security here considered as the combination of confidentiality that is how to prevent an unauthorized disclosure of information, integrity, prevention of unauthorized amendment or deletion of information and availability, the prevention of unauthorized withholding of information.

3. Literature Survey

Number of data security models have been developed to address the data security issues in cloud computing. The data security model using Two-Way handshake is a method which utilizes the homomorphic token with distributed verification of erasure-coded data and achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s)[3]. Sobol sequence method rely on erasure code for the availability, reliability of data and utilize token precomputation using Sobol Sequence to verify the integrity of erasure coded data rather than Pseudorandom Data in existing system, this scheme provides more security to user data stored in cloud computing. The performance analysis shows that scheme is more secure than existing system against Byzantine failure, unauthorized data modification attacks, and even cloud server colluding attacks [4]. In public auditing to support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient[5].In RSA cryptosystem Research Paper, they have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm in paper [6]. Recently, the model which uses computational intelligence performance was proposed, computational intelligence (CI) is a mathematical modeling technique of cloud computing, which are vitally importance to simplifying the complex system and designing proactive and adaptive system in a dynamic and complex environment towards data security [7]. The semantic based access control model considers relationships among the entities in all domains of access control namely Subject(user), Object(Data/resource), Action(select, open, read, write) and so on, it is also shown how to reduce the semantic interrelationships into subsumption problem. This reduction facilitates the propagation of policies in these domains and also enhances time and space complexity of access control mechanisms[8]. Applying agents method introduces agents to data security module in order to provide more reliable services[9]. A novel third party auditor scheme a thirdparty auditor which affords trustful authentication for user to operate their data security in cloud. The obvious advantage of this scheme is that the cloud service provider can offer the functions which were provided by the traditional third party auditor and make it trustful. So it indeed reduces the constitution‟s complexity in Cloud Computing [10]. Ensuring data security is the common aim for all the above categories of security model.

4. Data Security Issues

As many are moving to cloud storages, there are many potential attacks attempted few of them are:

a) Denial of Service(DoS) attacks:
As cloud is shared by many users, DoS attacks much more damaging.
b) Side Channel attacks:
By placing a malicious virtual machine to a target cloud server an attacker can launch a side channels attack.
c) Authentication attacks:
There are many different ways to authenticate users, and methods used are a frequent target of attackers.
d) Man-in-the-middle cryptographic attacks:
It is carried out when an attacker places himself between two users.
e) Inside-job:
Here person, employee or staffs who have the knowledge of system can attack the cloud system.

Security aspects can be classified as data integrity, confidentiality, availability and privacy as show in figure below.

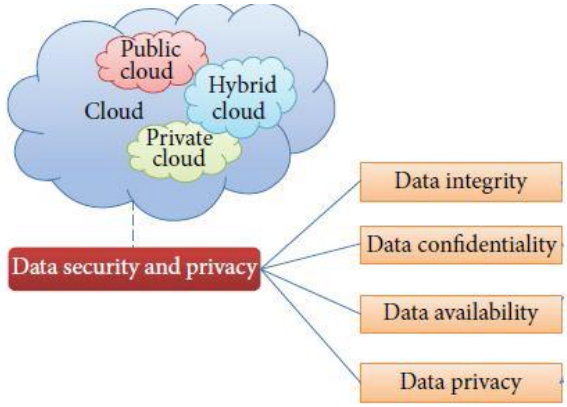

Figure (i): illustrates various data security concepts

Data Integrity
Generally data integrity means securing the data from unauthorized detection, fabrication or modification. It is one of the critical aspects in security. Data integrity in the cloud system means preserving information integrity. It is the basic to provide cloud computing service such as SaaS, PaaS and IaaS. [8]In cloud the data stored in data ware house must be secure enough from the intrusion and other damages. The loosing of data can be from inside or outside. While providing the security of data, cloud provider should implement mechanisms to ensure data integrity. He should make the client aware of what particular data is hosted on the cloud. There could e a malicious inside attack or from outside it could be hackers, attackers. Like Google docs got attacked in 2009, Amazon S3 was also attacked recently. In standalone system integrity is maintained via database constraints transactions. Access of data can be controlled by authorization.

Data Availability
It means the recovery of user‟s data when an accident such as hard disk crash, damage or any other network failures happens. The issue of storing data over servers is a main concern of user‟s as cloud vendors are governed by local laws and the cloud clients should be cognizant of those laws.

Data Confidentiality
User‟s privacy and confidentiality risks vary significantly with the terms of service and privacy policy governed by service providers. Data confidentiality is important for users who store their data private or confident data in the cloud. To ensure confidentiality in cloud data control strategies and Authentication are used. These issues can be addressed by increasing the cloud reliability and trustworthiness. Encryption is usually used to provide confidentiality for data.

5. Cryptography Methods

To secure the data which is uploaded by users into cloud, it has to be encrypted. Information in cloud data centers is encrypted by the users using many cryptography techniques.

Cryptography is the art and science of achieving security by encoding messages to make them non-readable". The plain text message is in simple English language that can be understood by any. The message is codified using cryptographies techniques called as cipher text message.

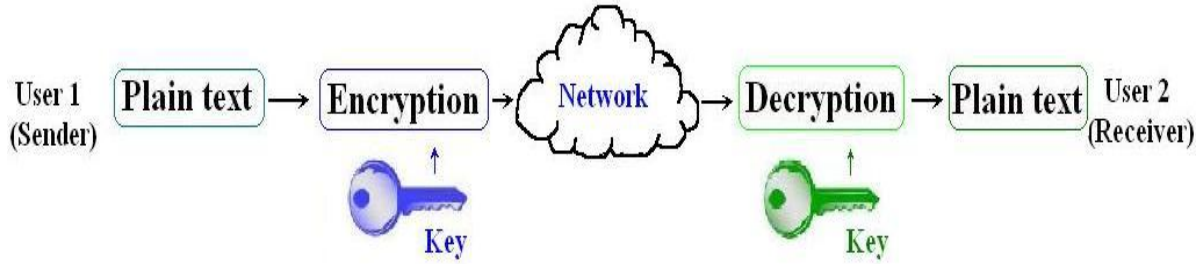

Figure (ii): illustrates Encryption and Decryption mechanism

We have three type of techniques 1) Symmetric Key Cryptography 2) Asymmetric Key cryptography 3) Hash function.

- **Symmetric Key Cryptography**

Symmetric encryption is the oldest and best-known technique. A secret key,which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

- **Asymmetric Cryptography**

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys-a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

- **Hash Function Cryptography**

The hash function cryptography (One way cryptography) offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one-way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages. The most used hash function cryptography techniques are: SHA1, MD5.

We can compare all these methods using various parameters. It is clear from the below table 1 that compared to symmetric and asymmetric, hash function has more advantages.

Table 1: Comparisons of all techniques

Metric	*Symmetric*	*Asymmetric*	*Hash*
Collision Resistant	NO	NO	Yes
Key agreement	Problem	No Problem but complex mathematical calculations	No problem
Complexity	Less	More complex	Less
Speed	Fast	Slow	Fast
Delays	Less	More	Less
Security	Less	Medium	High
Implementation	Difficult	Difficult	Simple

We can see that hash functions are less complex and simple to implement and at the same time very hard to break a hash function.

Cryptography relies on stable and unique key to encrypt and decrypt messages. As many cryptographic algorithms are be used in security like given below. The key point is that it is no longer adequate to simply encrypt your data. You must now actively select the appropriate cryptographic algorithms

Table 2: Famous Cryptography Algorithms

Type	**Algorithm**
Symmetric	DES, AES, RC5
Asymmetric	RSA, ECC
Hash	MD5, SHA1

Based on NIST and ANSI guidance, below table 3 provides the comparative strengths of various cryptographic algorithms. We try to look into how Various Hash function and ECC algorithms and how these can be used to protect the data in cloud computing.

Table 3: Comparing similar cryptographic algorithm strengths

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	Elliptic Curve Field Size	RSA Modulus Size
80 bits	2 Key Triple DES	SHA-1	160 bits	1,024 bits
112 bits	3 Key Triple DES	SHA-224	224 bits	2,048 bits
128 bits	AES-128	SHA-256	256 bits	3,072 bits
192 bits	AES-192	SHA-384	384 bits	7,680 bits
256 bits	AES-256	SHA-512	512 bits	15,360 bits

6. Proposed Algorithm and Implementation

In order to provide the safety and security assurance to the users data, we propose a Data security model that uses Elliptic curve cryptosystem for digital signature. Strength of the algorithm depends on the difficulty level of computing discrete logs in a large prime modulus. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient a reason to believe that the message was created by a known sender, and that it was not altered in transit. 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. In this work both digital signature scheme and public key cryptography are integrated to enhance the security level of Cloud. The encryption of digital signature into cipher text is done.

Proposed Algorithm

Step 1: In Digital Signature, the data/ document will be crunched down into few lines called as message digest by using hashing algorithm.

Step 2: The message digest is encrypted with private key to produce digital signature.

Step 3: Using Elliptic curve Algorithm, digitally signed signature is encrypted with receiver's public key.

Step4: Receiver will decrypt the digital signature into message digest using sender"s public key and the cipher text to plain text with his private key as shown in the fig (iii).

Digital signatures are important to detect forgery and tampering

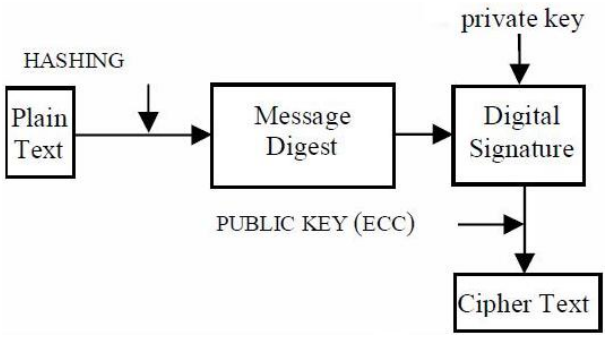

Figure (iii): Encryption of Digital Signature into Cipher text

Implementation

Elliptic Curve Crypto system works on principles of elliptic curve. The equation of an elliptic curve over a field K considered in our work is given as,

$$y2 = x3 + ax + b \quad (1)$$

where, x, y = co ordinates.
a, b = elements of K.

There are three steps in the process i.e., key generation, encryption and decryption.

Proposed Model

Key generation is an important part where we have to generate both public key and private key. The sender will be

encrypting the message with receiver‟s public key and the receiver will decrypt using its private key. Now, we have to select a number **'d'** within the range of **'n'**.

We can generate the public key Using the following equation.

$$Q = d * p \quad (2)$$

where, d = The random number that we have selected within the range of (1 to n-1).
P= the point on the curve.
Q = the public key and „d‟ is the private key.

Encryption
Let „m‟ be the message that we are sending. We 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 **C**1 and **C**2.

$$C1 = k * p \quad (3)$$
$$C2 = M + k * Q \quad (4)$$

Decryption
The message „M‟ that was sent is written as following equation,

$$M = C2 - d * C1 \quad (5)$$

Proof-
The message „M‟ can be obtained back using eq.(5)
C2 - d * c1 = (M + k * Q) - d * (k * p)
we have Q = d * p, by cancelling out k * d * p,
We get M (original message).

7. 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 below.

Table 4: 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:

- 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.

8. Results

The below Table 5 provides the key generation, as well as encryption and decryption times for ECC and RSA.

File Size (KB)	*Key Size (bits)*	*ECC Algorithm*				*RSA Algorithm*			
		Key Gen Time (ms)	*Encrypt Time (ms)*	*Decrypt Time (ms)*	*Size of Encrypted File (KB)*	*Key Gen Time (ms)*	*Encrypt Time (ms)*	*Decrypt Time (ms)*	*Size of Encrypted 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

9. Analysis of the 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(iv) 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. Fig2 shows the comparison of the key generation times for RSA and ECC.

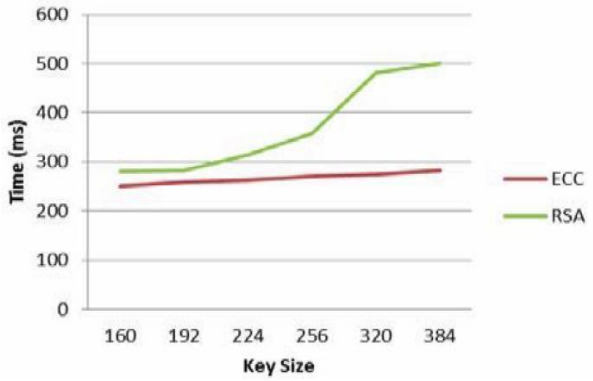

Figure (iv): illustrates Comparison of Key Generation Time

B. Encryption/Decryption Time
Figure (v) 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.

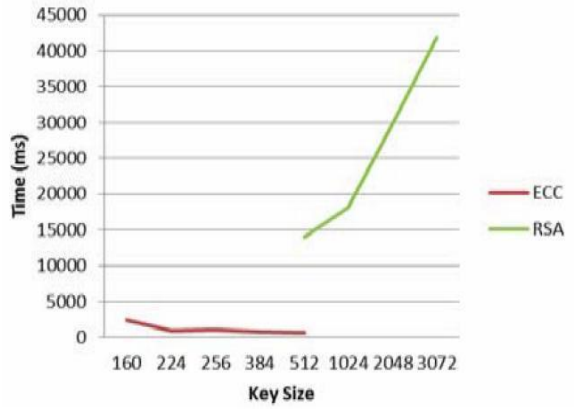

Figure (v): illustrates Comparison of Encryption Time

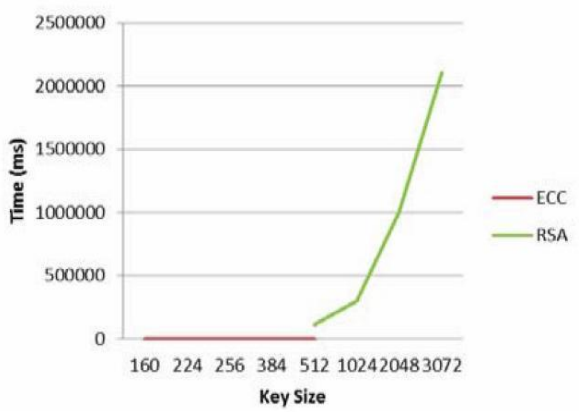

Figure (vi): illustrates Comparison of Decryption Time

Figure (vi) 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.

10. Acknowledgment

I would like to gratefully and sincerely thank my parents - father D.Chatur Naik and mother D.Ghammi Bai without whose unsustained support, I could not have completed this paper.

11. Conclusion and Future Scope

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

References

[1] Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
[2] RSA (algorithm), ttp://en.wikipedia.org/wiki/RSA_(algorithm)
[3] JavaTM Cryptography Extension (JCE), Reference Guide. http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCERefGuide.html
[4] Berta, I.Z., and Z. A. Mann. "Implementing Elliptic Curve Cryptography on PC and Smart Card", Periodica Polytechnica Ser. El. Eng. Vol 46. NO 1-2, PP 47. 2002.
[5] Brown, M., D. L. Hankerson, J. L_opez and A. Menezes. "Software implementation of the NIST Elliptic curves over prime fields". In Progress in Cryptology - CT-RSA, D. Naccache, Ed, vol. 2020 of Lecture Notes in Computer Science, pp. 250-265. 2001.
[6] Neal Koblitz, Alfred J. Menezes, "A Survey of Public-Key Cryptosystems". Advanced Computing & Communication Technologies (ACCT), Second International Conference, 2012.
[7] Certicom Corp. “An elliptic curve cryptography (ECC) primer”. White paper, Certicom. 2004.
[8] Rabah, K. "Implementation of Elliptic curve Diffie-Hellman and EC Encryption schemes". Information technology journal, 01/2005.
[9] Rabah, K. "Implementing Secure RSA Cryptosystem Using Your Own Cryptographic JCE Provider". Journal of Applied Science, vol. 6, Issue 3, p.482-510. 2006.
[10] Robshaw, M. J. B. and Y. L. Yin. “Elliptic Curve Cryptosystems”. 1997 http://www.rsasecurity.com/rsalabs/ecc/ellipticcurve.html

[11] Stallings, W. "Cryptography and Network Security: Principles and Practice, 3rd edition", Prentice Hall, New Jersey, 2003.
[12] Trappe. W and L. C. Washington "Introduction to Cryptography with Coding Theory", Prentice Hall, New Jersey, 2002.
[13] Weil, N. (1998). "U.S. govt.‟s encryption standard Cracked in record time „„. Network World. 1998, http://www.networkworld.com/news0720des.html
[14] Amara, M.; Lab. LAGA, Univ. Paris-8, St. Denis, France; Siad, A. "Elliptic Curve Cryptography and its applications".
[15] Fiskiran, A.M.; Dept. of Electronics Engg. Princeton Univ., NJ, USA, Lee, R.B. "Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments".
[16] S. Maria Celestin Vigila, K. Muneeswaran. "Implementation of Text based Cryptosystem using Elliptic Curve Cryptography".
[17] Ravi Shankar Dhakar, Amit Kumar Gupta, "Modified RSA Encryption Algorithm (MREA)". Advanced Computing & Communication Technologies (ACCT), Second International Conference, 2012.
[18] Suli Wang, Ganlai Liu, "File encryption and decryption system based on RSA algorithm". Computational and Information Sciences (ICCIS), International Conference, 2011.
[19] Maryam Savari, Mohammad Montazerolzohour and Yeoh Eng Thiam, "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application". Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference, 2012.
[20] P.R. Vijayalakshmi, K. Bommanna Raja, "Performance Analysis of RSA and ECC in Identity-Based Authenticated New Multiparty Key Agreement Protocol". Computing, Communication and Applications (ICCCA), International Conference, 2012.
[21] Kamlesh Gupta, Sanjay Silakari, "ECC over RSA for Asymmetric Encryption: A Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.
[22] Arjun Kumar, Byung Gook Lee, HoonJae Lee "Secure Storage and Access of Data in Cloud Computing". ICT Convergence (ICTC), International Conference, 2012
[23] Xiao Zhang, Hong-tao Du, Jian-quan Chen, Yi Lin, Leijie Zeng, "Ensure Data Security in Cloud Storage". Network Computing and Information Security (NCIS), International Conference, 2011.
[24] Somani, U, Lakhani, K, Mundra, M, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing". Parallel Distributed and Grid Computing (PDGC), 1st International Conference, 2010.
[25] 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.
[26] Depavath Harinath, “Net Neutrality- A Concept of Open Internet” in *International Journal of Science and Research*(IJSR),Vol.4, Issue 7, July 2015.
[27] Depavath Harinath, “Corpus of Internet Standards-The Standards for Communication” in *International Journal of Advanced Research in Computer Science* (IJARCS),vol.5, No. 3, March-April 2014.
[28] Vasanth.C.Bhagawat,Dr.A.Arul L.S.Kumar, “Survey on Data security Issues in cloud Environment”, in International Journal of innovative Research in Advanced Engineering (IJIRAE), vol.2, Issue 1. Jan. 2015.
[29] Depavath Harinath,et.al, “Enhancing Security through Steganography by using Sudoku Puzzle and ECC Algorithm” in International Journal for Research in Science Engineering and Technology(IJRSET) August 2015 Volume 2, Issue 6.
[30] Depavath Harinath,et.al, “Enhancing Security by using ECC Algorithm in Wireless Sensor Networks” in International Journal of Artificial Intelligence and Mechatronics(IJAIM) Volume 4, Issue 1. [2015]

Author Profile

Depavath Harinath, received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC. Accredited by NAAC with „A‟ grade and accredited by NBA, AICTE, New Delhi - Permanently Affiliated to JNTU, Ghatkesar, Ranga Reddy, Hyderabad, Telangana, India in 2012. Now working as Lecturer in Computer Science. Having four years of experience in teaching and already published 15 manuscripts in different international journals. Research fields includes Computer Networks and Network Security.