International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307 OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT239053

An efficient Technique for Data Security using Improved Elliptic Curve Cryptosystem over Cloud Computing

Sunil Manoi[1], S C Lingareddy[2]

[1,] Research Scholar, School of computer science and Engineering, REVA University, Bangalore India

[2] Professor, Computer Science and Engineering, SRI Venkateswara College of Engineering Technology Bengaluru, India

* Corresponding author's Email: sunil.manoli@reva.edu.in

ARTICLEINFO

Article History:

Accepted: 01 Sep 2023

Published: 08 Sep 2023

Publication Issue

Volume 9, Issue 5

September-October-2023

Page Number

57-65

ABSTRACT

Recent years have seen a rapid expansion of the cloud computing industry, which may be visualized as a distributed computing environment where cloud resources can be distributed shared. In comparison to traditional systems, there are thousands of computers operating in parallel, completing the specified task quickly. The parallel processing is made possible by the low cost of these virtualized hardware resources. In this paper, we discuss several cloud deployment options and how they differ from conventional computers in terms of security. Different methods that minimize the cloud and the limitations of current cryptographic techniques can be used to analyse this security. This research introduces ecliptic curve cryptography technique for various cloud-based applications and compares this technique with existing RSA algorithm-based applications to analyse the security in deployment models. The suggested elliptic curve based public key cryptography is shown to be superior to the current RSA algorithm based applications in this paper's experimental and theoretical results. Our experimental findings show that the suggested ECA approach outperforms the RSA algorithm. This aids in the use of security solutions for the various cloud computing deployment patterns that have been studied.

Keywords : Ecliptic Curve Cryptographic [ECC], RSA technique, deployment models, security techniques.

I. INTRODUCTION

The changing global scenario shows an elegant merging of computing and communication in such a way that computers with wired communication are being rapidly replaced to smaller handheld embedded computers using wireless communication in almost

every field. This has increased data privacy and security requirements. Data protection and authentication is now demanded for performing mobile banking on a cell phone, monitoring health of a patient through his wrist watch, remaining connected to office networks while travelling and so on. This has given a new thrust of what the technology guru Eddie Murphy has called the fourth wave – "Universal Connectivity" also termed as "Communication and Connectivity" by Embedded Market Forecasters. First three waves being defined as mainframe computers, PC revolution and Internet explosion respectively [1]. Data and information security is equally required along with other basic needs of reliable connectivity; high data transfer rate, optimised storage and processing etc.

Cloud computing is an umbrella term which involves different types of technology like distributed computing ,parallel programming ,grid technologies etc .Cloud computing provides tremendous opportunity for small and medium scale enterprises to grow their business using IT services with zero deployment cost.

Several authors have defined cloud in various ways .NIST defines Cloud Computing[1] as," Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.". Here technical aspects of cloud computing has been shown. According to Buyya [2] cloud can be defined as "A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers. ''. Clouds offer high scalable, elastic and resilient services on a pay-as-you-use model which can be utilized by the business houses for growing their business to reduce their infrastructure cost and power saving. Cloud provides flexibility and portability to its users.

Cloud based services are being used by small and medium scale enterprises to achieve greater speed in business processing and higher flexibility .Cloud Computing run on subscription based service model (pay as per you use) using internet as the infrastructure .Small and Medium Enterprises can set up the website and software on the cloud and hence get rid of the upfront infrastructure investments (cost incurred in purchasing and installing hardware, power and cooling cost and maintenance cost). This results in reduced cost of the services. Quality of services also gets better as the organization can spend the saved amount and time on improving it .With cloud based services innovative ideas can be easily implemented with reduced risk.

Cloud based software are playing same role in IT industry that banks are playing in finance sector .Cloud can manage our data as bank manages our fund. Cloud Computing runs on virtualization technology where multiple operating systems runs on a server .Clouds supports multi tenancy where multiple organization's data are stored on a single server using virtualization technology. Cloud computing is growing very rapidly due to availability of high speed internet .Web browser can be used to access software deployed on cloud computing which earlier used to get installed on the desktop. So users are able to access the same service at less cost or sometime totally free. These causes lot of transaction to happen on the network and hence security issues also rise along with them. Although cloud computing has evolved a lot, it has not won complete confidence of its user and it's being used mainly for experimental and testing projects. There are various reasons behind it and one of them is security of data stored on the cloud.

The rest of this paper is divided into literature review on deployment models and service models and various issues and security challenges face by cloud. Next section includes proposed method and followed by

results and analysis and ends this paper with proper conclusion and future work to be carried out.

II. LITERATURE REVIEW

This section describes the various survey on existing work done so far in the cloud computing. This literature review includes the analysis on various cloud deployment models and service models used and various challenges face by cloud computing in providing security.

2.1 Analysis of cloud deployment models

The cloud can be deployment in three different ways in the environment of cloud.

2.1.1 Public cloud: A service provider can host the cloud on its infrastructure and provide to other user for free or on pay-as-you-use-model. The user has to store its data outside its network so it cannot be used for storing private information. Multiple tenants may exist on the server which raises the security risk of data isolation. This is the most popular deployment model. Organizations like Google and Amazon provide services on this model.

2.1.2 Private Cloud: Private cloud is owned by a particular organization and only employees of the organization have the rights to access the cloud. Organizations have the freedom to define the protocol and access rights of its users though cloud could be managed by third party only. It's preferred for organization that have lot of sensitive data or government organizations

2.1.3 Hybrid Cloud: Hybrid cloud computing is mixed of publican private cloud. As public cloud can never be considered perfectly secure for sensitive data for them private cloud is used.

2.1.4 Community Cloud: It is very similar to grid computing were set of computers interoperates with each other to form network.

Private cloud has least security issues among the entire deployment model. They are completely owned by organizations. They are not multi-tenant in nature so they don't have privacy issues. These benefits come at the cost of investment on infrastructure and its maintenance. So they lack the major benefits that cloud computing can provide. On the other hand public cloud provides all kind of services and has maximum security issues and concerns. In this paper we are more concern about public cloud. If we can take care of public cloud, security issues of other kind of deployment model are taken care of.

2.2 Analysis of Cloud Service Model

There are three different kinds of service model for the cloud [3].

2.2.1 Software-as-a-service: Software is deployed on cloud and delivered as a service using web browser or as web services. User need not worry about buying hardware and installing software on them. SaaS applications need not be installed on the local machine and user does not have to worry about its update and maintenance. With SaaS vendors makes the required software available to a business on subscription basis and charges are made on product usage. SaaS model can save both infrastructure cost and operational cost. Database can be deployed on cloud on SaaS model but privacy hinders users from adopting it. In case of SaaS security related issues are completely handled by the providers.

2.2.2 Platform-as-a-service: It is application development and deployment platform deployed on cloud and delivered as a service. It also provides application programming interface, database and middleware to its user. The provider is responsible for maintenance and control of the underlying cloud infrastructure including network server and operating system. PaaS service provides great deal of flexibility allowing companies to build PaaS environment on demand with no capital expenditure. In case platform as a service security issues are handled by the provider partially and user or organizations need to add layer of security from their side

2.2.3 Infrastructure-as-a-service: Delivery of hardware along with basic software as a service falls in domain of infrastructure as a service e.g. storage as a service. With IaaS company can rent fundamental computing

resource for deploying and running or storing data. It enables companies to deliver applications more efficiently by removing the complexity involved with managing their own infrastructure. IaaS enables fast deployment of applications and improves the agility of services by instantly adding computing processing power and storage capacity when needed for example Amazon ec2. Moreover server failure and network failure are taken care of by the vendors while security concerns arising out of applications and web services are managed by the user.

2.3. SECURITY ISSUES OF CLOUD COMPUTING

A cloud computing based service faces various kinds of security challenges. An intruder can use the vulnerabilities of network infrastructure to attack the services on cloud .Characteristics of cloud like multi-tenancy; on demand self-service, broad network access etc creates lot of vulnerabilities in the service delivered [5]. A survey conducted by IDC shows that security is major concern for the users staying away from the cloud [6]. In this section we analyze various kind of security challenges arise for applications deployed on cloud. They include both traditional security challenges and recent challenges which came into existence because of cloud computing [7][8][9].

Security Risk due to network infrastructure: Network infrastructure raises several security issues with the service being provided. Distributed Denial of Service attacks are performed to prevent the server from providing service to its user by sending uncountable request. A system on cloud can be hacked and used as base to perform dos attack on other machine. Attacker analyzes all packets passing through the system to gather important information's about the user. Port scanning [10] is done too find out the open port that can be used to get into the system. SQL injections are used to attack the cloud based database.

Security risk due to use of web services: Web services are vulnerable to several kinds of attacks. These vulnerabilities arise due to implementation mechanism and existing protocols in web services. There are as follows.

Buffer Overflows: Xml can be forced to call itself thereby overflowing the memory. This can trigger error message and hence application reveal information about itself

XML injections: XML injections can be used to insert a parameter into a sql query and let the server execute the data.

Sessions Hijacking: An attacker can hijack a soap message and obtain the session id thereby representing himself as an authenticated user to the server. Later on he can go on to perform some serious damage to server.

Security risk due to cloud characteristics: Security risk arises for services based on cloud due to its characteristics. Service user losses control over data as it is stored on other's server. It has to depend on the provider's security arrangement and its employees. A situation may arise where service provider might have to move to other provider or back to its server at different geographic location. Data stored on cloud gets locked in other's server and it's difficult to move them from one provider to another.

Most of the cloud service provider support multi tenancy. Isolation of data from other organization's employee residing on the same server is also a challenge for the service provider. If client ceases to use the service provided than data ownership issues do arises as some provider refuses to release them.

Security issues of applications available through cloud: Applications deployed on cloud can face same kind of attacks as that on client-server model.

SaaS based applications are vulnerable to the virus .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 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. It gets divided into two parts when loaded from the memory. Deliver their services to user.

They face security challenges arising out of network infrastructure and web services .IaaS and PaaS services are hardware dependent and face more, challenges

arising out of characteristics of cloud computing, than SasS applications. Public key cryptography is one of the various ways to handle some of the issues. There are various kinds of public key cryptographic schemes. Elliptic curve cryptography is one of them

III. PROPOSED METHOD

The proposed method presents elliptic curve cryptography technique for providing security in cloud computing. In proposed ECC discrete points on the elliptic curve over a finite field are used as a cyclic group. All type of public key cryptography based schemes can get implemented using elliptic curve cryptography. Elliptic curve cryptography gives same level of security as other cryptographic schemes provide but it has not gained same popularity. It is based on group theory and field theory. Its security is based on elliptic curve discrete logarithm problem [13]. The results are drawn based on the Elliptic Curve Cryptography (ECC) technique which is mainly used for the instantiate of public key cryptography, consider for the instance executing of keys and digital signatures. There are various numbers of motivations behind energy of using elliptic can be used to find more possible solutions.[11].

ECC is a kind of open cryptosystem like RSA. Be that as it may, its snappier advancing limit and by giving appealing and option approach to specialists of cryptographic calculation influences it to contrast from RSA. A similar security level gave by RSA, can be additionally given by ECC, that likewise with littler key sizes. For example, the 2048 bit security strength of a RSA could be reduced to 326 bit security strength of ECC with the same level. \

This ECC technique we use for multiplication operation, which has been found to be computationally more efficient than RSA exponentiation. ECC results has drawn much attention as the security solutions for wireless networks such as Clouds, due to the small key size and simplified computation [13]. Elliptic curve has a unique property that makes it fit for use in cryptography in cloud computing i.e. its power to take any two points on a specific curve, add them together and get a third point on the same curve.

3.1 The algorithm of proposed ECC

The general equation for an elliptic curve which used to analyze the results is:

$$y2 + axy + by = x3 + cx2 + dx + e$$

Where a, b, c, d and e are real numbers and x and y belongs to a set of real number. In its simplest form, an elliptic curve equation can be given as:

$$y2 – x8 + dx + e$$

In this paper ECC discrete points on the elliptic curve over a finite field are used as a cyclic group. All type of public key cryptography based schemes can get implemented using elliptic curve cryptography.

Elliptic curve cryptography gives same level of security as other cryptographic schemes provide but it has not gained same popularity. It is based on group theory and field theory.

3.1.1 Overview of ECC

Elliptic Curve Cryptography (ECC) is the public key cryptography approach used for data encryption. This technique is used to solve major issues of public key cryptography by providing high level security with less key length. An Elliptic Curve is a plane curve defined by an equation

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

A standard form of elliptic curve A over finite field Bp (p is a large prime number) is computed by using the following equation

$$A: y2 = x3 + ax + b \pmod p \qquad (2)$$

Then, the procedure involves choosing two non-negative integers a, b which are less than p such that, it satisfies the condition

$$4a3 + 27b2 \pmod p \neq 0 \quad (3)$$

a. Operations of ECC for elective curve

If S(x1, y1) is a point on an elliptic curve, then its inverse is given by -S(x1, y1). The following equation is used to calculate the inverse [7].

$$-S(x1, y1) = S(x1, p-y1) \quad (4)$$

❖ Point Addition

Point addition is one of the elliptic curve arithmetic operations, When the two points of a curve P(x1, y1) and

Q(x2, y2) are distinct (P≠ Q), then P+Q is given by the

$$- \quad 3 = - \qquad 1 - 2 \qquad (6)$$

❖ Point Doubling

Point doubling is one of the basic elliptic curve arithmetic operations. When the two points of a curve P(x1,y1) and Q(x1, y1) overlap (P = Q), 2P.

❖ Scalar Multiplication

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition [7].

$$kP = P + P + P + \ldots + k \text{ times} \qquad (9)$$

Let us consider the elliptic curve over Fp where a=1, b =1 p =11 with the equation (1)

$$\text{Now, } y2 = x3 + x + 1 \pmod{11}$$

The set of solutions are E= {(1,10), (1,1), (3,5), (3,6), (4,2), (4,9), (6,4), (6,7), (8,3), (8,8), O}, including the point infinity O.

Elliptic curve point addition shows as follows:

By given points, P = (1,1) and Q = (8,8)

$$= (8-1) / (8-1) \bmod 11 = 1$$

P + Q = (1,1) + (8,8)

$$x3 = 12 - 1 - 8 = -8 = 3$$

$$y3 = 1(1-3) - 1 = -3 = 8$$

P + Q = (1,1) + (8,8) = (3,8)

If the selected point P be (8,8), then the doubling operation is performed as follows.

$$=(3 * 82+ 1) / (2 * 8) \bmod 11$$

$$=(50/ 5) \bmod 11 = 10$$

$$x3 = 102 - 2 * 8 = 84 \bmod 11 = 7$$

$$y3 = 10 (8 - 7) - 8 = 10 -8 = 2$$

2P = (8,8) + (8,8) = (7,2)

The result of point addition and point doubling is (3,8) and (7,2), because the elliptic curve points are in Abelian group.

General functions for ECC is as follows:

(i) Both sender and receiver agrees to send publicly-known data items. For this the following steps are followed

a) In elliptic curve equation, values of a and b and prime p

b) Points (elliptic group) computed from the elliptic curve equation

c) A base point Btaken from the elliptic group

(ii) Each user generates public or private key pairs using the following steps

a) Private key (d): an integer x, selected from the interval [1, p-1]

b) Public key (Q): product of private key and base point Q = d*B

❖ Key Generation

Step 1: Both sender and receiver agree with the base point P

Step 2: Private key = d, public key Q = d * P

i. Encryption

Step 1: Select a elliptic curve Ep (a, b). E has N points on it

Step 2: Plain text has to represent on the curve

Step 3: Randomly select'd' from [1-(n-1)]

Step 4: Consider message 'm' has the point 'M' on the curve 'E'

Step 5: Two cipher texts will be generated C1 = d*P, C2 = M + d*Q

The nature of super increasing order is hidden by vector v1usingmodular multiplication and a permutation, and then the super increasing vector is represented by v. The distorted vector forms the encrypted message. The original super increasing vector forms the private key which is used to decipher the message.

IV. RESULTS AND DISCUSSION

The results are drawn in this paper based on considering the parameters based on the size of the key and comparing the key size with different types of security methods.

The below table-1 describes the comparison of ECC key size and equivalent RSA key size [13].

Type	ECC Key Size	RSA Key Size	Ratio
Type-1	112	512	1:5
Type-2	163	1024	1:6
Type-3	192	1536	1:8
Type-4	224	2048	1:9
Type-5	256	3072	1:12
Type-6	384	7680	1:20

Table 1: Comparison of sizes with keys

The proposed ECC algorithm is implemented and RSA algorithm in an environment similar to the existing cloud techniques. The proposed ECC technique is implemented in real cloud system named as miles web cloud.

Our simulation results shown in figure-3 shows clearly that proposed ECC performance is better than RSA when it is compared considered. Key generation algorithm is compared described in Figure -4 shows overall performance of two different algorithms.

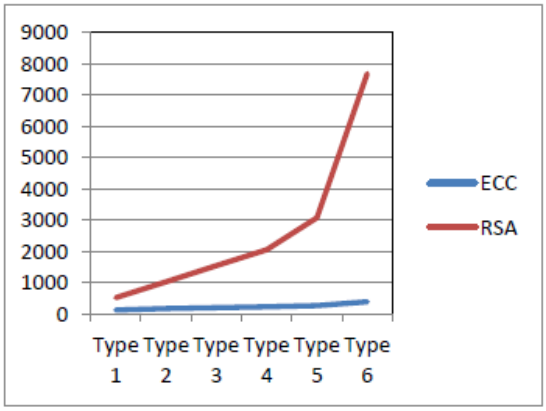

Figure 3: comparison of growth RSA vs proposed ECC on types

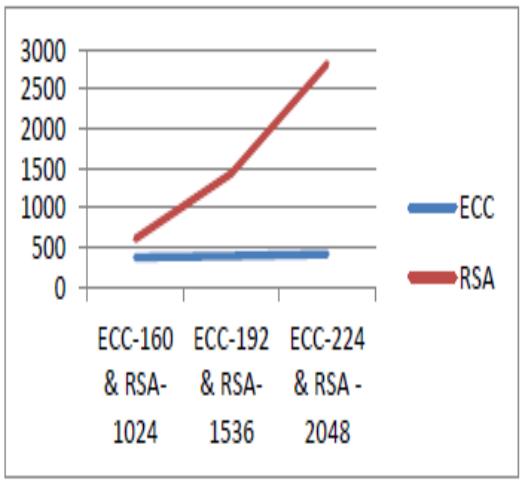

Figure 4: Key comparison vs RSA and Proposed ECC

V. ANALYSIS

A Statistical investigation, demonstrates that a similar level of security rendered by a RSA-based framework with a huge modulus can be proficient with a considerably smaller elliptic curve group, i.e. a 163 piece key of ECC is thought to be as secure as 1024 bits key in RSA. Also ECC uses smaller key sizes, which effects in faster calculations, lower power consumptions, saving memory and bandwidth ECC thus clubbed with Cloud computing will definitely provide much more secure environment along with speed and saving of many intangible/indirect resources. ECC applied in cloud will result in more attention paid towards how to avoid data duplications, how to utilize data and services efficiently and how to achieve cost-effective solutions.

VI. CONCLUSION AND FUTURE ENHANCEMENT

This paper concludes the Cloud Computing for the service-based architecture is utilized. The community of the cloud must take the dedicated measures to ensure in providing best security. The present trend continues to adopt various standards to ensure interoperability among different service providers. The proposed ECC can be also used as a part of mobile computing and encryption technique in server side, encryption of images and their application in the field of different applications. In cloud computing the propose cryptographic technique can be describes as new area in the context of research where the data security is the main concern to provide the security and the confirmation on the data between the user and the service providers. the future the modified ECC techniques can be used to optimize the cloud for the optimizing the resources of the cloud and this ECC techniques is clubed with other resource allocation technique and can be used to optimize the resources.

VII. REFERENCES

[1]. S. Subashini, V. Kavitha -Anna University Tirunelveli, India," A survey on security issues in service delivery models of cloud computing "ELSEVIER- Journal of Network and Computer Applications Volume 34, Issue 1, January 2011, Pages 1–11.

[2]. Jashanpreet Pal Kaur, Rajbhupinder kaur, Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab, "Security Issues and Use of Cryptography in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014, ISSN: 2277 128X.

[3]. Wang, L., Tao, J., & Kunze, M. (2008). "Scientific cloud computing: Early definition and experience". Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Austin, TX, 825–830.

[4]. Reservoir Project [URL]. http://www-03.ibm.com/press/us/en/pressrelease/23448.wss/, access on June 2008.

[5]. Amazon Elastic Compute Cloud [URL]. http://aws. amazon. com/ ec2, access on Nov. 2007.

[6]. IBM Blue Cloud project [URL]. http://www3.ibm.com/press

/us/en/pressrelease/22613.wss/, access on June 2008.

[7]. Nimbus Project [URL].http://workspace.globus.org/ clouds/nimbus.html/,access on June 2008.

[8]. Status Project [URL]. http://www.acis.ufl.edu/vws/, access on June 2008.

[9]. OpenNEbula Project [URL].http://www.opennebula.org /, access on Apr.2008.

[10]. Shweta Sharma, Bharat Bhushan, Shalini Sharma - "Improvising Information Security in Cloud Computing Environment"- International Journal of Computer Applications (0975 – 8887) Volume 86 – No 16, January 2014.

[11]. D. J. Bernstein and T. Lange (editors). eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench. crypto, October 2013.

[12]. Dr.R.Shanmugalakshmi, M.Prabu – "Research Issues on Elliptic Curve Cryptography and Its applications"- IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[13]. Wang, H., Sheng, B. and Li, Q. (2006) 'Elliptic curve cryptographybased access control in sensor networks', Int. J. Security and Networks,Vol. 1, Nos. 3/4, pp.127–137.

[14]. Ms Bhavana Sharma, B.P.I.T., Rohini, Delhi- "security architecture of cloud computing based on elliptic curve cryptography (ecc)" ICETEM 2013.

[15]. Wikipedia, the free encyclopedia of Cloud Computing.

[16]. Lim, I, Coolidge, E, Hourani, P, (2013) Securing Cloud and Mobility: A Practitioner´s Guide, USA, CRC Press.

[17]. Yong yu,Liang Xue,Man Ho Au,Willy Susilo, Jianbing Ni,Yafang Zhang,Athanasios V. Vasilakos,Jian Shen," Cloud data integrity checking with an identity-based auditing mechanism from RSA".

[18]. 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.

[19]. 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.

Cite this article as :

Sunil Manoi, S C Lingareddy, "An efficient Technique for Data Security using Improved Elliptic Curve Cryptosystem over Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 5, pp.57-65, September-October-2023. Available at doi : https://doi.org/10.32628/CSEIT239053
Journal URL : https://ijsrcseit.com/CSEIT239053