May – June 2020
ISSN: 0193-4120 Page No. 7295 - 7298

ECC based Encryption and Decryption using Cloud

Kajol Ki Naidu[1], Adarsh Krishnan[2]
[1]Student ,SRM Institute of Science and Technology, Kattankulathur
[2]Student, SRM Institute of Science and Technology, Kattankulathur
Kajol_p@srmuniv.edu.in[1], adarshkrishnan_kutty@srmuniv.edu.in[2]

Article Info
Volume 83
Page Number: 7295 - 7298
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

***Abstract*:**
The Elliptic curve cryptography is a form of cryptography[6], which uses public key that is computationally harder to implement yet faster, and provides better security when compared to the widely used RSA or AES cryptography. What makes the ECC encryption algorithm better is its smaller key sizes which save up on computing time. The formula for finding the keys is complex. That's why breaking the encryption is much more difficult.In our paper, through the research on the basic working of the elliptic curve encryption algorithm, we have come up with an optimized method from the perspective of data protection in cloud and it has been designed using the elliptic curve encryption algorithm with data protection in cloud technology to ensure that the system is running safely and efficiently [2], where the data is encrypted when sent and stored in the cloud and can be downloaded and decrypted in a similar way.

Indexterms:Cloud, Elliptic Curve Cryptography, ECC Encryption , Decryption[5]

I. INTRODUCTION

The objective of our project is to use ECC encryption algorithm to encrypt and decrypt the data using cloud[4].
Cloud computing helps users to simply store their data and easily share data with others. Thanks to the safety threats in an untrusted cloud server, users are recommended to compute verification to their data to guard the integrity. The degree of the information security that the cloud computing platform is under, directly affects the user's data security problem. Therefore making cloud security very important and relevant in today's world.[2]
The phrase computer security or the term security refers to the techniques used to make sure that the stored data inside a computer can not be compromised or be read by any individual without any authorization from the users. Data encryption stands for the translation of knowledge into a form that's unintelligible to a layman without using a deciphering mechanism. Computer security measures these days involve encoding, encrypting and passwords which all lean towards cryptography.
Cryptography is the art of hiding information or data within a writing that does to make sense when looked at by a layman. But, when it's decoded, it holds information or a message. It's of two types basically:- symmetric key also known as private-key cryptography and asymmetric key also known as public-key cryptography. Symmetric-key cryptography consists of systems, which encrypt and decrypt and provides only confidentiality whereas when comparing an asymmetric-key cryptography technique, it provides integrity, authentication and confidentiality of travelling and the storage of the message. Albeit symmetric key cryptography is much more efficient and faster than asymmetric key cryptography, it faces difficulties in key management and key distribution. Comparing this with asymmetric key cryptography, itprovides a way to avoid key distribution and finds a way to distribute key and key management problems of symmetric-key cryptography.

May – June 2020
ISSN: 0193-4120 Page No. 7295 - 7298

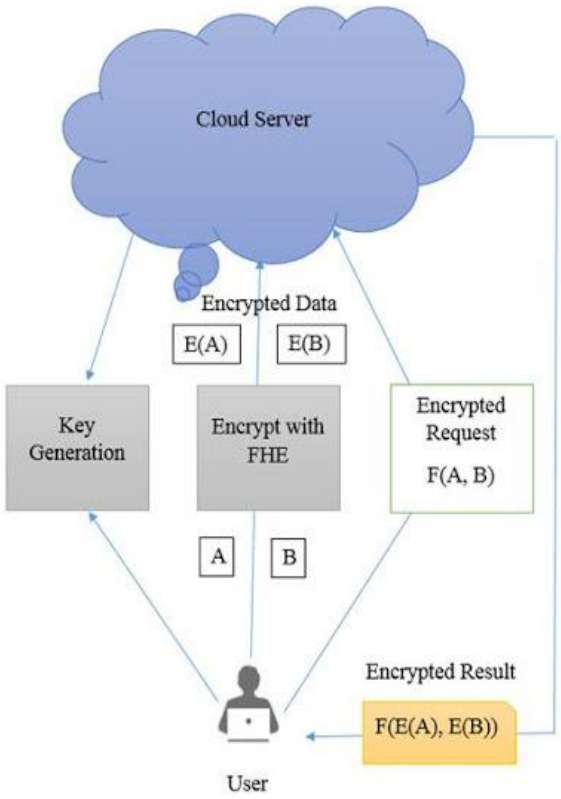

Fig.1 Encryption on Cloud.

The use of Elliptic Curve Cryptography is currently not popular as the RSA as ECC is much more complex to implement. ECC encryption uses smaller key sizes when compared to the ever popular RSA encryption algorithm.
Although ECC has a smaller key size, the security is much more when compared to RSA due to the Elliptic curve way of selecting the keys which make it very secure as ut cannot be broken/hacked easily.

II. BASIC WORKING OF THE PROJECT:

ECC stands for Elliptic curve cryptography. The key features of ECC that makes it stand out are:
Elliptic curve cryptography is an asymmetric encryption algorithm, which is done using high level complex calculations using elliptical curves to encrypt as well as to decrypt the data. RSA is a similar encryption algorithm which is also asymmetric. The difference between RSA and ECC is that the ECC uses a smaller key size when compared to RSA. ECC encryption algorithm in comparison with the other present algorithms is better even though its much more complex due to its smaller key size which means lesser computation power used to encrypt and decrypt data.[4]\

The process of ECC encryption algorithm takes place in the following way:

1. Define a Curve to use
2. From the defined curve, we generate a key pair, one public and the other private for the sender as well as the receiver.
3. From the key pair that has been generated, we generate another secret shared key.
4. Generate an encryption key from the shared secret key and use that to encrypt the data.
5. Using the encryption key that we have generated and the symmetric encryption algorithm, we encrypt the data .

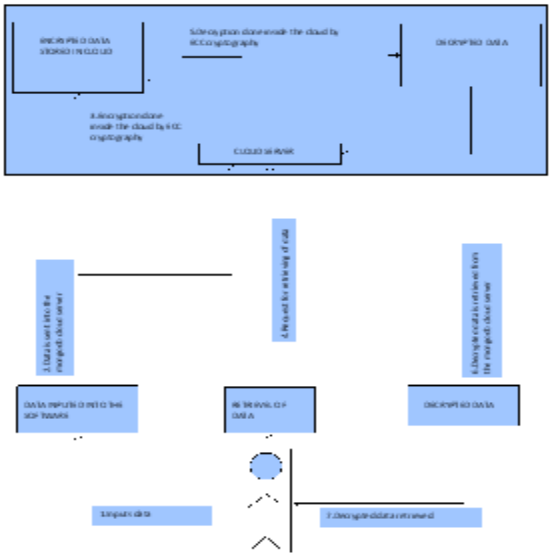

Fig. 2 Architecture Diagram

The Decryption is as follows:
The sender will have to share their public key with the receiver. The sender will also have to either share the curve that was chosen to compute the encryption to the receiver or ,the sender and receiver will have to have the same use for the same curve type. The decryption takes place as follows:

1. From the same curve that we've used, generate another public and private key pair to be used by the receiver.
2. From the private key of the receiver and the public key of the send, we generate another shared secret key.
3. To help decrypt the data, another encryption key is generated from the shared secret key.

May – June 2020
ISSN: 0193-4120 Page No. 7295 - 7298

III. PROPOSED WORK

When the data is uploaded into the cloud server, the data is first encrypted using ECC encryption and stored into the database server. Upon retrieval from the database, the data is first accessed by the system and the decryption process takes place. Here, various measures such as "Encryption Time " ,"Average Execution Time", "Average Delay Time", "Average Overhead time" and "Decryption Time" is calculated and presented[7].

A comparison of the calculated values is made with the conventional encryption algorithm values to depict proof of ECC encryption being faster than AES or RSA.

IV. EQUATIONS

The given below equation and graph depicts the encryption as well as the decryption of the data and key generation from the graph[8]

$y^2=x^3+ax+b$ (1)

)

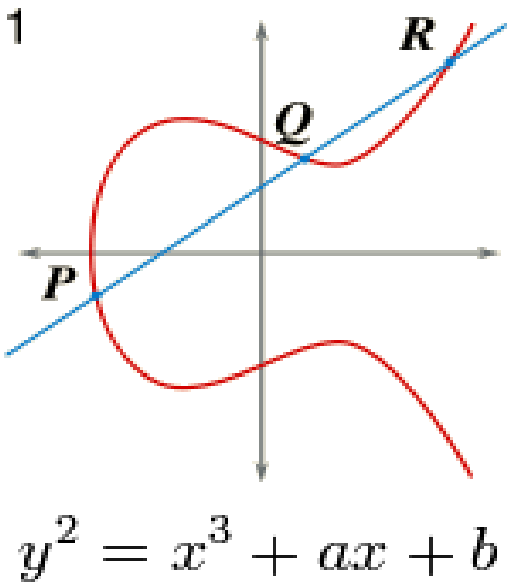

Fig. 3 Simple Elliptic Graph with Equation

The public key is given by

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

Encryption is given by

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

Decryption is given by

$$M = C2 - d * C1^{[1]} \quad (5)$$

E is the curve.
Q is the calculated public key from the graph
P is a point taken on the curve.
d is a private key[9].
n is maximum limit.
M is the point taken on the curve.
k is a number selected at random between 1 to (n-1)[10]

VI. RESULTS DISCUSSION

The ECC algorithm was executed and the input data was encrypted. Different data was input and the subsequent results which followed are :

Out of whichof Fig 4 is the GUI of our project

Fig 5and Fig 6 shows the difference between encryption and decryption time when compared to RSA.

Fig 7 and Fig 8 shows comparison of encryption time between ECC and RSA cryptography.

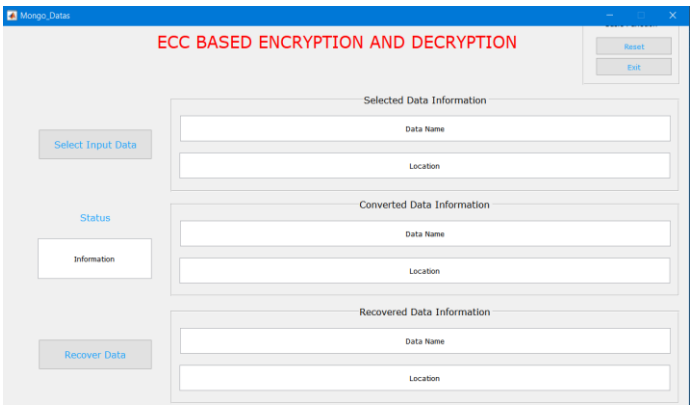

Fig. 4 The user interface used to show the output is given.

May – June 2020
ISSN: 0193-4120 Page No. 7295 - 7298

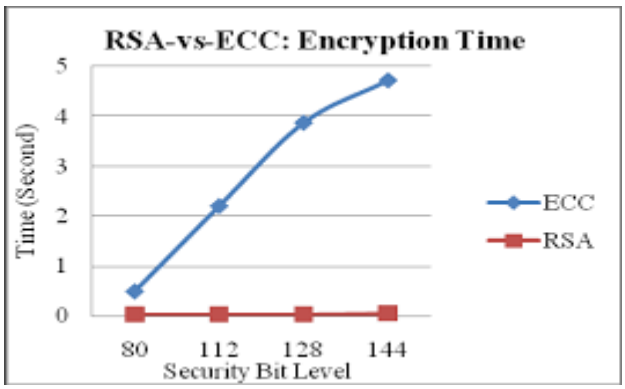

Fig. 5 ECC VS RSA Encryption Time Comparison

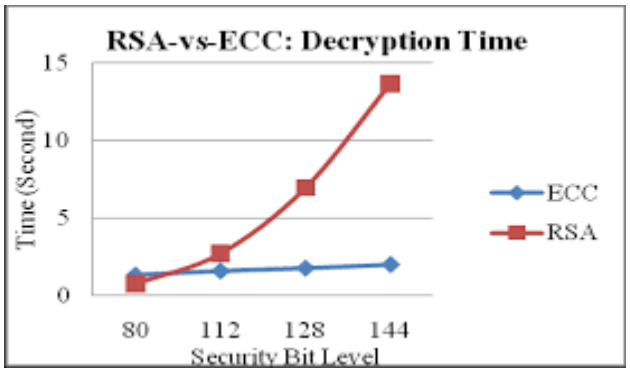

Fig. 6ECC VS RSA Decryption Time Comparison

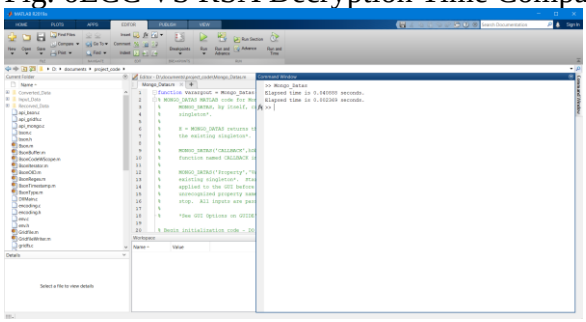
Fig.7 Result of time taken for a .txt file.

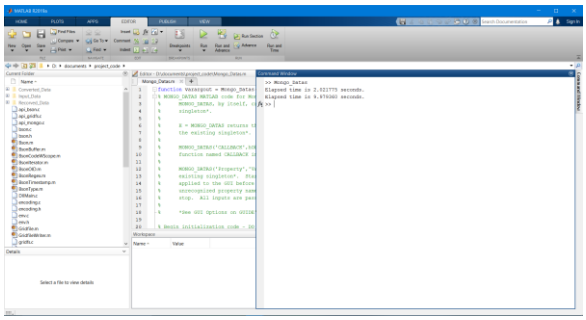
Fig. 8 Result of time taken for a pdf file.

VI.CONCLUSION

In this project the ECC encryption algorithm is used and executed, as well as ,compared with the conventional RSA algorithm to see how ECC works when compared to the typically used RSA and AES.

The results prove right in showing how ECC is better although it takes a little longer time in encrypting and decrypting the data.

VII. REFERENCES

[1]. Bruno F. Ferreira, Ney L. V. Calazans. "A flexible soft IP core for standard implementations of elliptic curve cryptography in hardware", 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems (ICECS), 2013

[2.]Feng Sheng Wu. "Research of Cloud Platform Data Encryption Technology Based on ECC Algorithm", 2018 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), 2018

[3]. "Advances in Computer, Communication and Control", Springer Science and Business Media LLC, 2019

[4]."Emerging Technologies in Data Mining and Information Security", Springer Science and Business Media LLC, 2019

[5]. N. Sathishkumar, K. Rajakumar. "A Study on Vehicle to Vehicle Collision Prevention Using Fog, Cloud, Big Data and Elliptic Curve Security Based on Threshold Energy Efficient Protocol in Wireless Sensor Network", 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), 2017

[6]"Emerging Trends in Computing and Expert Technology" Springer Science and Business Media LLC, 2020

[7].M. Thangavel, P. Varalakshmi, Mukund Murrali , K. Nithya. "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)", Journal of Information Security and Applications, 2015

[8] Feng Tian. "Application and Research of Mobile E-commerce Security Based on WPKI", 2009 Fifth International Conference on Information Assurance and Security, 08/2009

[9] "Computing and Network Sustainability", Springer Science and Business Media LLC, 2019

[10]. R. Bhuvaneswari, R. Ramachandran "Prevention of Denial of Service (DoS) attack in OLSR protocol using fictitious nodes and ECC algorithm", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017