International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 2, 2022 ISSN: 2348-6600
Reference ID: IJCS-395 PAGE NO: 2719-2721

Security using Elliptic Curve Cryptography (ECC) in Cloud

Mohamed Amin Abdiaziz Hussein[#1], Dr. A. Sivakumar[*2]
[#]*Student, M.Sc Information Technology, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021*
mohamedaminabdiazizhussein.mit20@rathinam.in

[*]*Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021*
sivamgp@gmail.com
ORCID iD: https://orcid.org/0000-0003-3517-816X

Abstract - **The Elliptic Curve Cryptography (ECC) is modern family of public-key cryptosystems, you can use an elliptic curve algorithm for public/private key cryptography. To be able to use ECC; cryptographic signatures, hash functions and others that help secure the messages of files are to be studied at a deeper level. It implements all major capabilities of the asymmetric cryptosystems: Encryption, Signatures and key exchange. The main advantage is that keys are a lot smaller. With RSA you need key servers to distribute public keys. With Elliptic curves, you can provide your own public key. Using public key cryptosystems with both public & private key can give security for data compare to single key encryption. In this project ECC algorithm is used for security data to cloud and uploading data to cloud.**

Index Terms - **Elliptic Curve Cryptography, Encryption, RSA, Public, Private Key.**

I. Introduction

With the invention of cloud, the days of keeping all your documents, photos, music files etc. on your computer's hardware is 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. 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 is 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.

II. System Study

Existing system:

AED, DES are mostly used crypto graphic algorithms for securing data. These methods are used in most of the applications which use single key for encryption & decryption.

Disadvantages:

1. These methods are old methods which are used in most of the applications.
2. They use single key for encryption & decryption

Proposed system:

In cloud environment data security is very important as data is stored in third party servers there is need to effective multi key encryption techniques like ECC algorithms. In this project we are using ECC algorithm in python language and using cloud to store encrypted data.

Advantages:

1. Time taken for encryption process is less.
2. Multiple keys are used for encryption & decryption process.

III. Module Details

In the proposed system contains the following modules,

1. Upload File
2. Encrypt File Using AES
3. Encrypt File Using ECC
4. Outsource File to Cloud
5. Download File

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 2, 2022 ISSN: 2348-6600
Reference ID: IJCS-395 PAGE NO: 2719-2721

6. Comparison Graph

Upload File: using this module we will upload any file to application

Encrypt File Using AES: using this module we will read file data and then encrypt it using AES algorithm and then compute encryption time

Encrypt File Using ECC: using this module we will encrypt file using ECC algorithm and then calculate encryption time

Outsource File to Cloud: using this module we will outsource file to cloud server for storage

Download File: using this module we will send file request to cloud and then download and decrypt the file

Comparison Graph: using this module we will plot encryption time graph between AES and ECC algorithm

IV. Literature Survey

Since their introduction to cryptography in 1985, elliptic curves have sparked a lot of research and interest in public key cryptography. In this essay, we present an overview of public key cryptography based on the discrete logarithm problem of both finite fields and elliptic curves. We discuss one of the basic and important properties of elliptic curves, the group law, and show that the set of points on the curve forms an additive abelian group. We show how the order of this abelian group affects the discrete logarithm problem and hence the security of a public key cryptosystem. We present the Diffie-Hellman key exchange and El Gamal cryptosystem based on the discrete logarithm problem of finite fields and also give their analogues in the elliptic curve case. We finally show why elliptic curves are dictating the future of public key cryptography and what makes them more efficient in constrained and wireless communications.

Enhanced public auditability & secure data storage in cloud computing

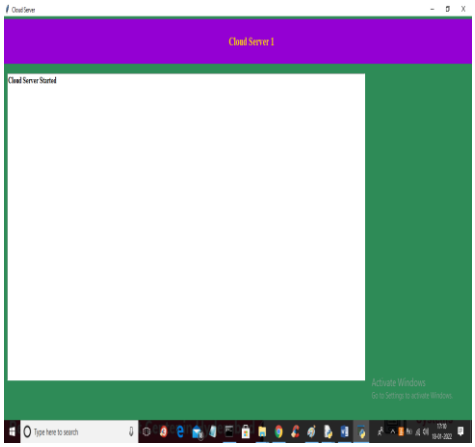
Cloud computing is the most envisioned paradigm shift in the computing world. Its services are being applied in several IT scenarios. This unique platform has brought new security issues to contemplate. This paper proposes a homomorphic encryption scheme based on the Elliptic curve cryptography. It implements a provable data possession scheme to support dynamic operation on data. The application of proof of retrievability scheme provisioned the client to challenge integrity of the data stored. The notion of a third-party auditor (TPA) is considered, who verifies and modifies the data on behalf of the client. Data storage at the server is done using a Merkle hash tree (MHT) accomplishing faster data access. This proffered scheme not only checks the data storage correctness but also identifies misbehaving servers. The initial results demonstrate its effectiveness as an improved security system for data storage compared to the existing ones in most prospects.

New Directions in Cryptography

Kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

V. Output Screens

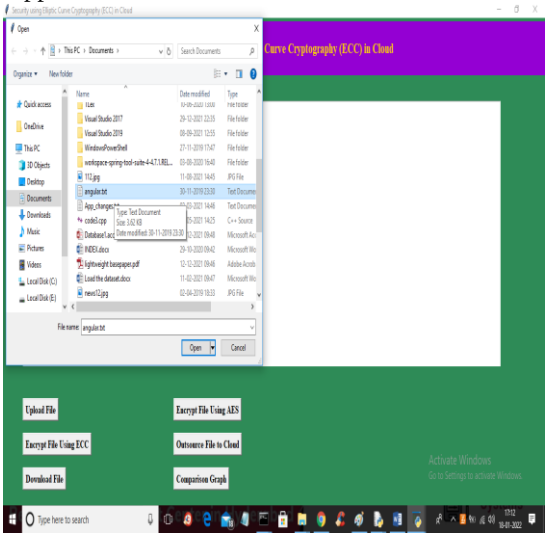
To run project first double click on 'run.bat' file from 'cloud Server' folder to start cloud application and to get below screen.



In above screen cloud server started and now double click on 'run.bat' file from 'Cloud User' folder to start cloud user application and to get below screen

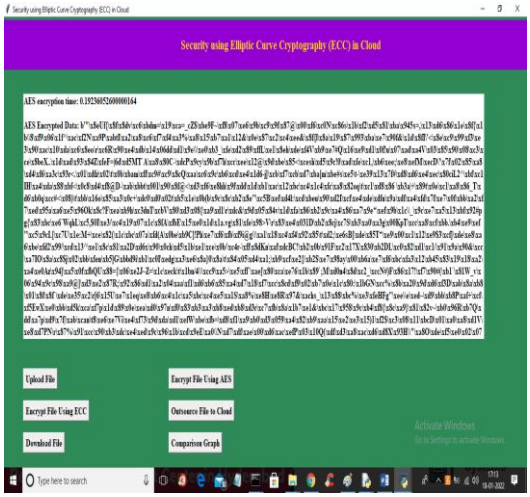
International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 2, 2022 ISSN: 2348-6600
Reference ID: IJCS-395 PAGE NO: 2719-2721

In above screen click on 'Upload File' button to upload any file to application like below screen



In above screen selecting and uploading 'angular.txt' file and then click on 'Open' button to load file and to get below screen

In above screen file is loaded and now click on 'Encrypt File Using AES' algorithm button to encrypt file and to get below screen.



In above screen we can see plain data is encrypted and in first line AES encryption time is 0.192 milli seconds. Now click on 'Encrypt File using ECC" button to encrypt same file using ECC and calculate time.

VI. 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.

REFERENCES

[1] Elliptic curve cryptography, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography.
[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.