ISSN 2277-2685
IJESR/Apr-Jun. 2024/ Vol-14/Issue-2/1335-1343
Mrs.A.Anitha Reddy *et. al.,* / International Journal of Engineering & Science Research

ELLIPTIC CURVE CRYPTOGRAPHY (ECC) BASEDFILE ENCRYPTION FOR CLOUD STORAGE

[1] **Mrs.A.Anitha Reddy,**
Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, Anitha.a@sreyas.ac.in

[2] **Mamidi Praful Reddy,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,mamidi.prafulreddy1@gmail.com

[3] **Prerana Ganji,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,ganjiprerana1531@gmail.com

[4] **Bhoomi Sushma,**
Department of CSE, Sreyas Institute of Engineering and Technology,Telangana,India, sushmabhoomi2002@gmail.com

[5] **Ramagala Naveen Kumar,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, Naveenkumar63025@gmail.com

Abstract

Cloud computing is one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing is Internet based computing due to shared resources, software and information are provided to consumers on demand dynamically. Cloud computing is one of the fastest growing technologies of the IT trade for business. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper will explore data security of cloud in cloud computing by implementing encryption with elliptic curve cryptography.

keywords: *cloud computing, cloud security, elliptic curve cryptography, datasecurity.*

I INTRODUCTION

A A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving

resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser. However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing provided

II LITERATURE SURVEY

***Elliptic Curve Cryptography for Securing Cloud Computing Applications*.**

Computing applications and data are growing so rapidly that increasingly larger servers and data center are needed for fast processing within the required time. A fundamental shift in the way Information Technology (IT) and computing services are being delivered and purchased results in the development of cloud computing. The out-of-control cost of power in terms of electricity generation, personnel hardware and limited spaces in data centers have encouraged a significant number of enterprises to move more infrastructures into a third party provided Cloud. However, Cloud computing requires that organizations trust that a service provider's platforms are secured and provide a sufficient level of integrity for the client's data. 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. An important factor is the key strength, i.e. the difficulty in breaking the key and retrieving the plain text. In this paper, we proposed Elliptic Curve Cryptography scheme as a secure tool to model a Secured platform for the Cloud Application.

A Secured Cloud Security Using Elliptic Curve Cryptography.

Cloud Computing is a modern paradigm which enables utilization of pool of computing resources in the

most proficient way. This emerging technology provides great opportunity in support of small and medium scale business houses to grow their business using the computing IT resources with no deployment cost. Cloud computing with well-built security has become a boon in the field of Information Technology. Cloud security is becoming a key differentiator and competitive edge between cloud providers. The prime responsibility of the cloud services provider is assuring security and integrity of the consumer's data. The lack of trust on data security is being the key obstacle to the IT sectors to move their data to the cloud. Lot of researches has been done to improve the performance of cloud data security. Hence cloud computing is still discovering several security issues. The high-quality cloud security can be achieved by efficient encrypting techniques. In this paper, we projected a model using Elliptic Curve Cryptography (ECC) to provide efficient data security in Cloud computing.

Design and Implementation of Enhanced Secured Cloud Computing.

Cloud computing plays a major role in providing different resources in the form of web services like tax calculation web service, e-banking web service etc., for smooth running of our daily lives. We can rely on cloud computing if these useful web services are really secure enough to use. This paper focuses on analyzing limitations of current cryptographic schemes used in providing security to data on cloud and highlights the usage of Elliptic Curve Cryptography scheme (ECC) used in cloud-based applications and implements Elliptic curve digital signature algorithm on cloud data and compares its performance with RSA based scheme. The performance of elliptic curve cryptosystem heavily depends on an operation called point multiplication. In this paper a new point multiplication method using modified base representation is used. This method reduces the point addition as well as pint doubling operations thereby increasing the efficiency of computing time in performing encryption and decryption operations.

Enhancing Security Using ECC in Cloud Storage

Due to its smaller key sizes and quicker computations when compared to conventional public key cryptography algorithms, ECC is a subset of public key cryptography that has grown in popularity. The paper investigates the foundations of ECC. The article also covers several popular ECC algorithms. With the help of the Elliptic Curve Cryptography algorithm, this work aims to provide security services like confidentiality for cloud services. Because of its benefits in terms of smaller key sizes, less CPU time, and less memory usage, it should be used for data encryption rather than the well-known and widely used

RSA algorithm. This survey paper provides an overview of the key concepts and applications of (ECC).

Implementation of Text Encryption using Elliptic Curve Cryptography

Elliptic Curve Cryptography has been a recent research area in the field of Cryptography. It provides higher level of security with lesser key size compared to other Cryptographic techniques. A new technique has been proposed in this paper where the classic technique of mapping the characters to affine points in the elliptic curve has been removed. The corresponding ASCII values of the plain text are paired up. The paired values serve as input for the Elliptic curve cryptography. New technique avoids the costly operation of mapping and the need to share the common lookup table between the sender and the receiver. The algorithm is designed in such a way that it can be used to encrypt or decrypt any type of script with defined ASCII values.

III EXISTING SYSTEM

Cloud computing platforms provide an opportunity for users to securely store and retrieve their data. Cloud computing faces many challenges, which makes users worry about using it to store their huge data and applications in the cloud. One of the prime challenges of the cloud is security. AES encryption, a widely adopted symmetric encryption algorithm, serves as the cornerstone for data security in cloud environments. Its implementation involves the use of varying key sizes to encrypt and decrypt data.

Disadvantages

Large Key size

Computational Complexity

Vulnerable to Quantum Attacks

Implementation

IV PROPOSED SYSTEM

All existing algorithms require large keys and heavy computation time, which may increase cloud usage costs. To overcome this problem, the ECC (Elliptic Curve Cryptography) algorithm is introduced, which uses small keys compared to others and takes less computation time to encrypt or decrypt data. This method uses point multiplication, which is multiplying the points of an elliptic curve with an unknown

exponential value, which gives a new point on the curve, which is then combined with the original data to form encrypted data. This process is reversed to decrypt the data. This work aims at improving cloud computing within cloud organizations with encryption awareness based on Elliptic Curve Cryptography.

Advantages

Less Encryption Time

Scalable

Less Complex Implementation

Harder to Decrypt

Uses Less Computational Power

V IMPLEMENTATION

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 AESalgorithm and then compute encryption time

Encrypt File Using ECC: using this module we will encrypt file using ECC algorithm and thencalculate 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 anddecrypt the file

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

To implement this project, we have designed two different applications

Cloud Server: This is a python-based cloud server which accept input file from user and then save in its storage space. Any time user can send request to download particular file and cloud will respond to user with that file. All files send to this cloud will be encrypted using ECC.

Cloud User: cloud user will upload file and then encrypt using ECC and then send or outsourceto cloud for storage. Any time user can send request to cloud for file download and then decryptit.

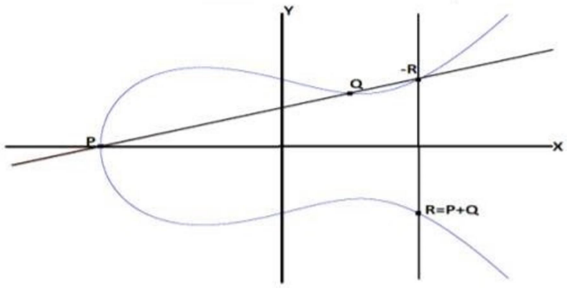
Algorithm

ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation:

$Y^2=x^3+ax+b$

along with a distinguished point at infinity, denoted "∞". (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated). This set together with the group operation of the elliptic group



theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the

divisor group of the underlying algebraic variety.

If P and Q are on E, R = P + Q

As shown in Fig.2, Let P=(x1,y1), Q=(x2,y2)R=(x3,y3) and P not equals Q

$$m = \frac{y_2 - y_1}{x_2 - x_1};$$

To find intersection with E, we get(m(x-x1)+y1) 2=x3+Ax+B

Or, 0=x3 -m2 x2 +.....

So, x3=m2 -x1 -x2y3=m(x1 -x2)-y1

Elliptic curves are used as an extension to other current cryptosystems. ECC is considered as more secured algorithm than other asymmetric algorithms such as RSA and Diffie-Hellman by providing same level of security with smaller key size. For example, ECC can provide a level of security with a 256-bit public key that other techniques require a 3072-bit public key. Thus ECC has some advantages include low CPU consumption, low memory usage and greater speed. The difficulty of discrete logarithm makes ECC so important.

VI CONCLUSION

Cloud computing is one of the most important research domains nowadays, with unmatched potential to improve scalability, optimize resource allocation, and streamline computing processes. Its rapid adoption across a variety of industries is supported by its Internet-based architecture, which makes it easier for users to dynamically access shared resources, software, and information as needed. But because cloud computing is open and distributed, security must be taken seriously because privacy issues and data breaches make it difficult for the technology to be widely used. As such, the necessity of addressing cloud computing security has become central to industry and university research initiatives. The purpose of this paper is to further this discussion by delving into the topic of data security in cloud computing, with a focus on elliptic curve cryptography-based encryption. It is envisaged that this investigation will contribute to strengthening cloud computing's security infrastructure, which will support the technology's ongoing expansion and advancement in the digital world

REFERENCES

[1] Alowolodu O.D, Alese B.K, Adetunmbi A.O., Adewale O.S " Elliptic Curve Cryptography for Securing Cloud Computing Applications" International Journal of Computer Applications (0975
– 8887) Volume 66– No.23, March 2013

[2] Karthik Sundararaj , Dr.M.Gobi, "A Secured Cloud Security Using Elliptic Curve Cryptography" UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015

[3] M. Gayatri "Design and Implementation of Enhanced Secured CloudComputing" International Journal of Electronics Communication and Computer EngineeringVolume 5, Issue

2, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

[4] Tejaswi Kumbhar, 1Rahul Gaikwad, 2Srivaramangai R "ENHANCING SECURITY USING ECC IN CLOUD STORAGE" © 2023 IJCRT | Volume 11, Issue 6 June 2023 | ISSN: 2320- 2882

[5] Laiphrakpam Dolendro Singh∗ and Khumanthem Manglem Singh " Implementation of Text Encryption usingElliptic Curve Cryptography" Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[6] Ayman Helmy Mohamed, Aliaa A.A. Youssif, Atef Z. Ghalwash " Cloud Computing Security Framework based on Elliptical Curve" International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 15, January 2015.

[7] Abhuday Tripathi, and Parul Yadav, Enhancing Security of Cloud Computing using Elliptic Curve Cryptography, International Journal of Computer Applications, 57(1), 2012, 0975-8887.

[8] Nilesh N. Kumbhar, Virendrasingh V. Chaudhari, and Mohit A.Badhe, The Comprehensive Approach for Data Security in Cloud Computing: A Survey, International Journal of Computer Applications, 39(18), 2012, 0975-8887.

[9] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, 1987.

[10] Yubo Tan, and Xinlei Wang, Research of Cloud Computing Data Security Technology, 978-1- 4577- 1415-3/12,IEEE 2012.

[11] Yashpalsinh Jadeja, and Kirit Modi, Cloud Computing - Concepts, Architecture and Challenges, International Conference on Computing, Electronics and Electrical Technologies,4(12), 2012, 978-1-4673-0210

[12] Dr. Chander Kant, and Yogesh Sharma, Enhanced Security Architecture for Cloud Data Security, International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 2013.

[13] Wayne Jansen, and Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, U.S. Department of Commerce, 800-144.

[14] Veerraju Gampala, Data Security in Cloud Computing With Elliptic Curve Cryptography, International Journal of Soft Computing and Engineering (IJSCE), 2, 2012.

[15] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, and Tang Chaojing, Data Security Model

for Cloud Computing, Proc. International Workshop on Information Security and Application. Qingdao, China, 2009, 978-952-5726-06-0.

[16] Ikshwansu Nautiyal, and Madhu Sharma, Encryption Using Elliptic Curve Cryptography Using Java as Implementation Tool, International Journal of Advanced Research in Computer Science and Software Engineering, 4(1), 2014. [11] Vidyanand K\Ukey, and Nitin Mishra, Dataset Segmentation for Cloud Computing and Securing Data Using ECC, International Journal of Computer Science and Information Technologies, 5(3), 2014, 4210-4213.

[17] R. Bala Chandar, and M. S. Kavitha, A Proficient Model For High End Security in Cloud Computing, ICTACT Journal of Soft Computing, 04(02), 2014.

[18] Nina Pearl Doe, and Sumaila Alfa, An Efficient Method to Prevent Information Leakage in Cloud, IOSR Journal of Computer Engineering (IOSR-JCE) 16(3), 2014, 2278-8727