ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12 Issue.1Jan 2024

SECURITY USING ELLIPTIC CURVE CRYPTOGRAPHY IN CLOUD

[1] Tasneem Rahath , [2]Jeevana katta, [3]Joshitha Kancharla, [4]Jyothsna poreddy

[1]Assistant professor in Department of Information Technology Bhoj Reddy Engineering College for Women

[2,3,4] UG Scholars in Department of Information Technology Bhoj Reddy Engineering College for Women

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 technology 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.

I INTRODUCTION

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.

II LITERATURE SURVEY

Research of Cloud Computing Data Security Technology

With cloud computing applications and research at home and abroad continue to advance cloud computing platform for users and data exchange between the greater the amount of user data transmission and storage a security threat, a cloud computing security is an important issue to be resolved. In this paper, all with state of encryption technology, presents a cloud computing data security solutions, both to ensure safe transmission of data to ensure the security of static data.

An Efficient Method to Prevent Information Leakage in Cloud

Cloud Computing is storing and accessing data and programs over the Internet instead of personal computers. It is a computing paradigm shift where computing is moved away from personal computers or an individual server to a cloud of computers. Its flexibility, cost-effectiveness, and dynamically re-allocation of resources as per demand make it desirable. As desirable as it is, it has also created security challenges such as information leakage, account hijacking and denial of service. The proposed work is to develop a Software as a Service application to prevent information leakage by providing multifactor authentication, risk assessment, encryption using enhanced elliptic curve cryptography where a cryptographically secure random number generation is used to make the number unpredictable, data integrity, key management and secure disposal of information. The platform for deployment of the application is Google App Engine.

Enhancing Security of Cloud Computing using Elliptic Curve Cryptography

Cloud computing is a form of distributed computing environment. It provides an environment where thousands of computers work in parallel to perform a job in much less times than traditional client server model. This parallelism happens because of low cost virtualization of hardware resources. Cloud computing abstracts the complexity of services provided to the user. In this article we have tried to explore various cloud computing model and how their security requirement differs from traditional computing model. We have analyzed various security risk associated with them, different ways to mitigate them and limitations of current cryptographic schemes. We have analyzed elliptic curve cryptographic schemes for cloud based applications in comparison to RSA based schemes. Here we have tried to give theoretical and experimental results to proof that elliptic

curve based public key cryptography is far better than RSA based schemes. We have implemented ecdsa algorithm and compared its performance with RSA based algorithm in cloud. It supports our conclusion from the survey of cloud based applications.

The Comprehensive Approach for Data Security in Cloud Computing: A Survey

Cloud Computing is becoming next stage platform in the evolution of the internet. It provides the customer an enhanced and efficient way to store data in the cloud with different range of capabilities and applications. The data in the cloud is stored by the service provider. Service provider capable and having a technique to protect their client data to ensure security and to prevent the data from discloser by unauthorized users. This paper, will gives a descriptive knowledge regarding cloud computing privacy and security issue provided by encryption and decryption services. If a cloud system is performing a task of storage of data and encryption and decryption of data on the same cloud then there are much more chances of getting access to the confidential data without authorization. This increases the risk factor in terms of security and privacy. This paper helps us on proposes a business model for cloud computing which focused on separating the encryption and decryption service, from the storage service provided by service provider. I means that both encryption and decryption of the data can performed at two distinct places. For studying this proposal are using a business model named as CRM (customer relationship model) for an example. For the evaluation of effective an efficient technique of data storage and retrieval we are providing three clouds separately such as including encryption and decryption services, secondly storage and a CRM application system. In this Research paper, we have tried to access separate encryption and decryption service using RSA algorithm and computing is a paradigm in which information is stored in servers on the internet. That information retrieved by the client as per usage. For this manner, we provide us a solution for data security, confidentiality and privacy based on a concept of separate encryption and decryption service.

Enhanced Security Architecture for Cloud Data Security

Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be main security threat. So, it is the responsibility of cloud service providers to ensure privacy and security of data on storage as well as network level. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on cloud environment is maintained or not. The proposed work is to define cloud architecture with configured samba storage and cryptographic encryption techniques. The cloud architecture deployed with samba storage uses

operating system feature specifying permission values for three attributes (User/Owner, Group and Global) and maps it to cryptographic application which performs cryptographic operations. Cryptography application supports symmetric and asymmetric encryption algorithm to encrypt/decrypt data for uploading/downloading within cloud storage. A username and password based authentication mechanism for users and digital signature scheme for data authenticity are defined within cloud architecture.

III EXISTING SYSTEM

Many of these challenges should be addressed through management initiatives. These management initiatives will requires clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer. Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Although proper security controls must be implement based on asset, threat, and vulnerability risk assessment matrices. Cloud computing security risk assessment report mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud.

Disadvantages

Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization.

IV PROPOSED SYSTEM

All existing algorithms require large size of keys generation and management which took heavy computation time and resources which may increase cloud usage cost and to overcome from this problem ECC (elliptic curve cryptography) algorithm is introduce which is lighter to generate keys and take less computation time and resources to encrypt or decrypt data.

The Cloud Computing systems that provide services to the Internet users apply the 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

Advantages

The need to access cloud storage on thin clients and mobile devices is becoming an emerging application.

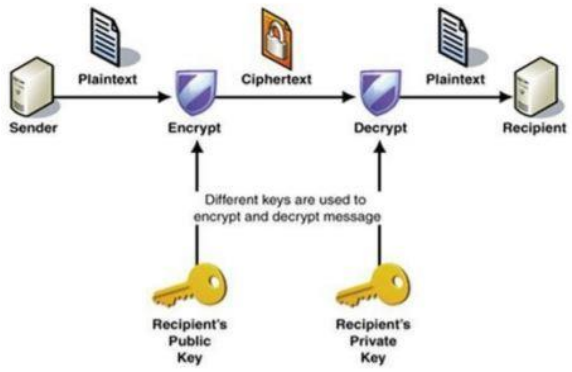
Security of stored data and data in transit may be a concern when storing sensitive data at a cloud storage provider.

V ARCHITECTURE

ISSN2321-2152

www.ijmece .com

Vol 12 Issue.1Jan 2024



VI IMPLEMENTATION

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 outsource to cloud for storage. Any time user can send request to cloud for file download and then decrypt it.

To implement this project we have designed following modules

1) ***Upload File***: using this module we will upload any file to application
2) ***Encrypt File Using AES***: using this module we will read file data and then encrypt it using AES algorithm and then compute encryption time
3) ***Encrypt File Using ECC***: using this module we will encrypt file using ECC algorithm and then calculate encryption time
4) ***Outsource File to Cloud***: using this module we will outsource file to cloud server for storage
5) ***Download File***: using this module we will send file request to cloud and then download and decrypt the file
6) ***Comparison Graph***: using this module we will plot encryption time graph between AES and ECC algorithm

VII ALOGRITHMS USED

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:

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

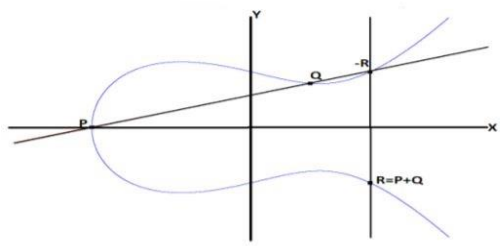
along with a distinguished point at infinity, denoted "∞". (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated). This set together with the group operation of the elliptic group theory form an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

ISSN2321-2152

www.ijmece .com

Vol 12 Issue.1Jan 2024

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

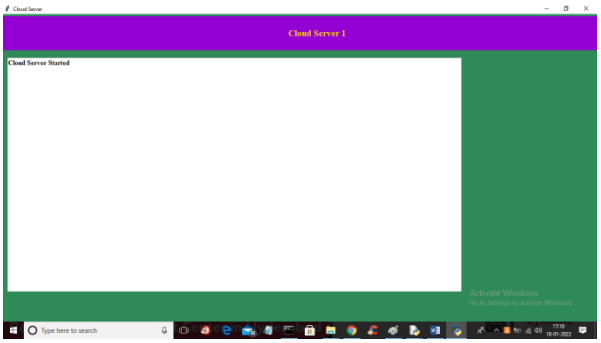
Or, 0=x3 -m2 x2 +.....

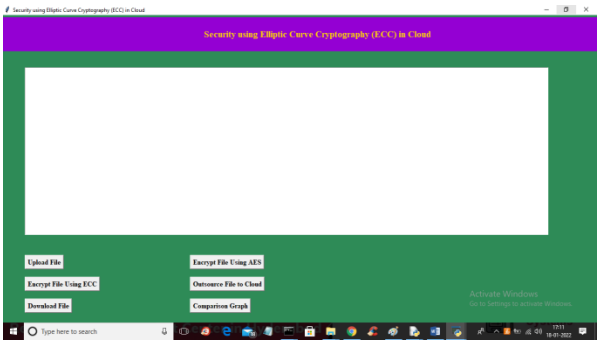
So, x3=m2 -x1 -x2

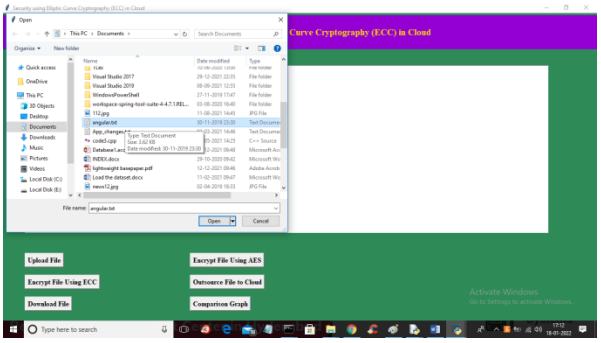
y3=m(x1 -x2)-y1

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.

VIII RESULTS



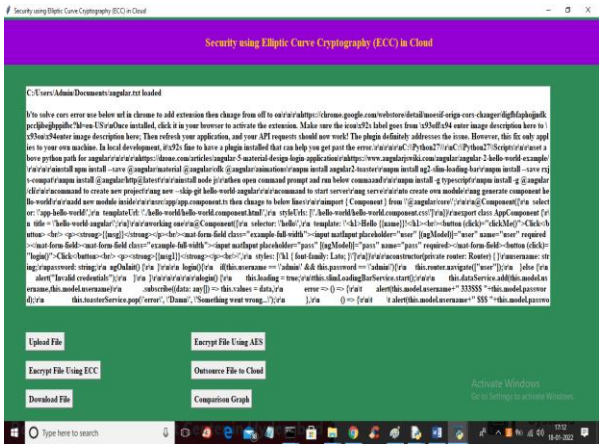


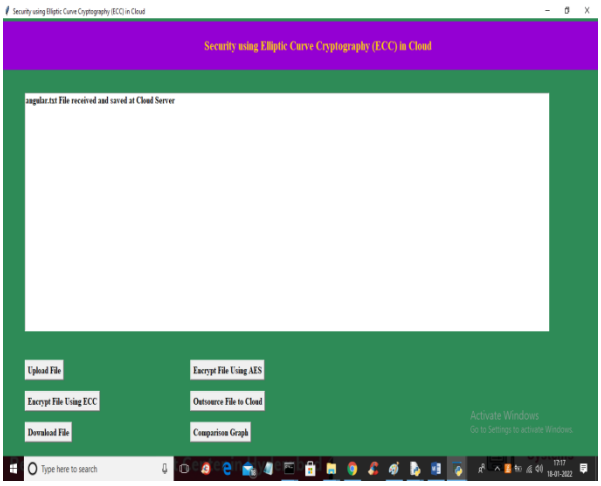


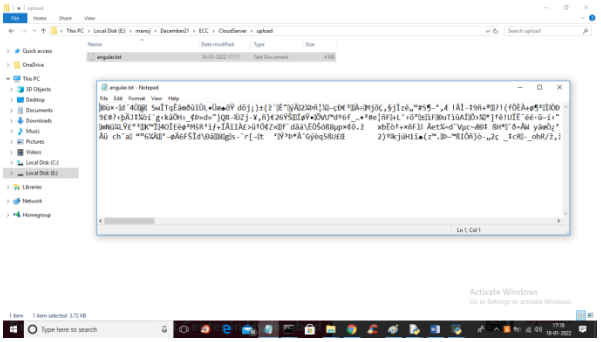
ISSN2321-2152

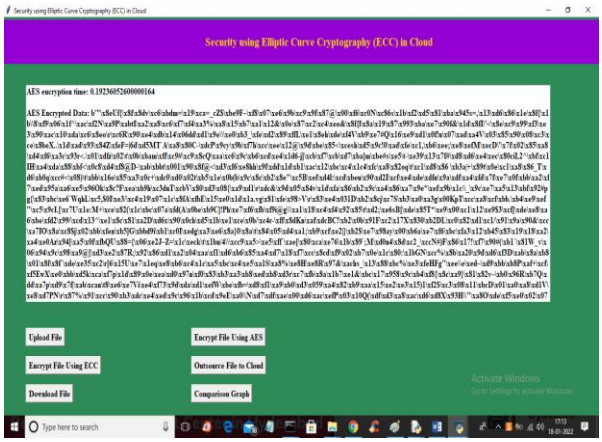
www.ijmece .com

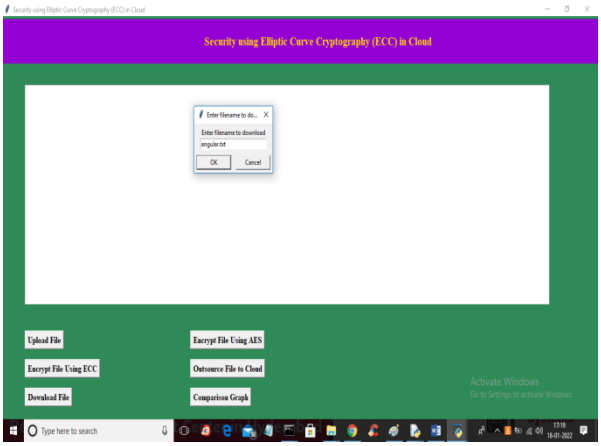
Vol 12 Issue.1Jan 2024

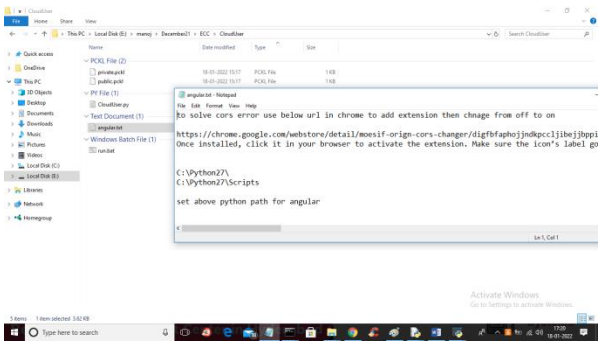


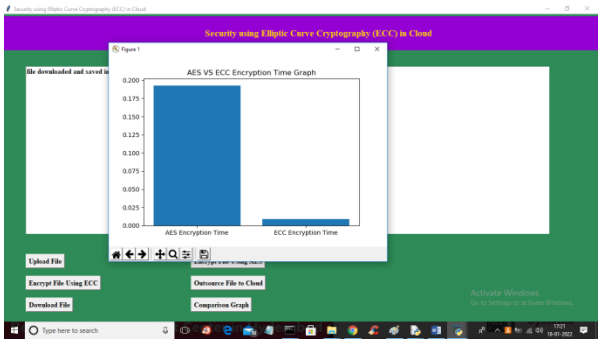


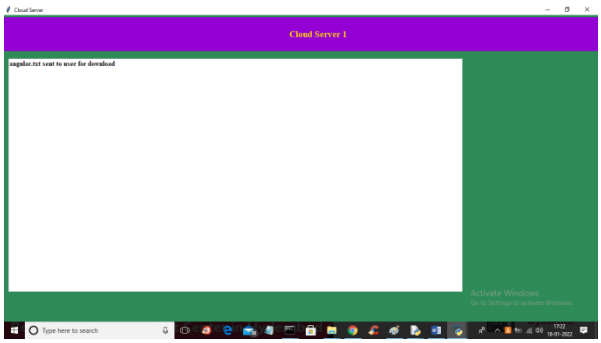












IX CONCLUSION

Cloud Computing provides a platform with an enhanced and efficient way to store data in the cloud. The functioning of Cloud Computing is significantly distressed by issues such as that of data security, integrity, theft, loss and presence of infected applications. These issues are the major disadvantages to the consumer to move their data to the cloud. This paper proposed a model using Elliptic Curve Cryptography to enable more efficient data security in the cloud computing. Here, Security is based on the difficulty of computing discrete logarithm in a finite field. AES and ECC are forms of public key cryptography, in which one decryption key, known as the private key, is kept secret, while another, known as a public key, is freely distributed. Public key cryptography is computationally more expensive than private key encryption, which employs a single, shared encryption key. By using the proposed algorithm, Cloud computing can achieve high level of security more than the security attain by the IT enterprises their own hardware and software.

REFERENCES

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

[2] 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.

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

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

[5] 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

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[12] 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.

[13] 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.

[14] Neha Tirthani, and Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, International Association for Cryptologic Research Cryptology ePrint 49, 2014.