Enhancing Security in Cloud Storage Using ECC Algorithm

Pankaj Sharma[1], Rohit Anil Singh[2], Niranjan Tiwari[3], Assistant Prof. Neha Jain [4]
[1, 2, 3, 4] Dept of Computer Engineering
[1, 2, 3, 4] Shree L.R. Tiwari College of Engineering, Thane

Abstract- *Cloud Computing is the approaching need of computing which is generally used for the IT Industries. Due to its many advantage such as flexibility, elasticity and optimal resource utilization the use of cloud computing is increasing day by day. Hence Security in cloud computing is an evolving area in today's world. It is subject of concern for Cloud Technology Services. One of the measures which cloud user can take care of is to encrypt their data before its stored on the cloud. This work is designed towards providing security service such as confidentiality in the cloud services. Since Application is also deployed on the Cloud and so for the secure transmission of the data we will be using Elliptic Curve Cryptography (ECC) algorithm instead of familiar and generalized RSA for data encryption because of its advantages in terms of smaller key sizes, lower CPU time and less memory usage.*

Keywords- elliptical curve cryptography, discrete logarithm problem.

I. INTRODUCTION

Cloud platform in practice is a use of a directory at inaccessible running an event on the Internet to store, manage, and process data choice using a local server or a personal computer. There are various major cloud service providers such as Google, Microsoft etc and others that are providing cloud computing services. Transmitting a data over cloud provides great facility to the cloud users because they do not have to care about the maintenance cost and management cost of the equipment. With so many great facilities Cloud also as drawbacks too. Once the client data is uploaded on cloud a major question that adposition the client is How secure the data is on cloud? This question Accor because the client loses his control over the data to Cloud Service Provider. Also the data now is on structured platform which is prone to various attacks. Now it becomes major concerns to ensure secret, integrity and availability of data on cloud .In order to provide secure data; most of cloud service provider use a combination of techniques including sanction, obscuring processes and sanction practices in their system. inconspicuous, which means they use a composite algorithm to inconspicuous information. To obscuring the encrypted files, a user needs an encryption key. Authentication processes, which require creating a user name and password. sanction practices in which the client lists the customer who are authorized to access information stored securely on the cloud network.

Cloud service providers operate large data centers, and customer who require their data to be hosted or buy or lease storage capacity from them. The data center worker,which are present in the backprocess, virtualizes the resources according to the requirements of the client and expose them as storage pools, which the client can themselves use to store files or data objects. Cloud storage services may be accessed through a web service API or through a Web-based user interface. The cloud storage architectures build a single virtual cloud storage system or cloud of clouds system The security in cloud is provided by various techniques such as Shamir, Data Encryption Standard **(**DES), D*iscrete Logarithm Problem (*DLP) and Rivest Shamir Adelman(RSA) algorithm etc. Hence, the point to be noted is that this traditional cryptographic algorithms are not practically much efficient in key generation time, encryption and decryption time and size of encrypted files. Also they require big integer computationco-processor to complete the calculations in a timely manner. Using such a co-processor significantly increase the cost of manufacturer, lead many devices impractical. This problem is overcome by using Elliptic Curve Cryptography (ECC), has become the cryptography of choice for mobile computing and communication devices due to its size and efficiency benefits.

II. LITERATURE REVIEW

Cloud storage is a storage model where data is not only stored in the client personal computer , but also in virtualize pools of storage which are generally or normally presented by outsider parties. This paper mainly concerns about management and security issues Accor with cloud computing and some serious security threats that prevails this field and management of the threads and attacks. The three professors in the computer science lab at MIT- Ronald Rivest, Shamir Adi and Adleman Leonard in year 1978 while working on developing acryptographic system for practical which is based on Diffie-Hellman (DH) proposition, they realized a fact that ,Its very simple and easy to multiply two prime numbers to get a large composite number, but on its reverse its difficult to take that composite number and find its prime number components . The output of this research is simply referred as RSA based on its inventor. This technique is one of the most powerful encryption technique used now a day.

In **[1] R. Gharshi, Suresh** proposed a system to provide a cloud and data security using ECC encryption technique. It used to prevent any unauthorized user try to access the private data to access the cloud. It was very noticeable that the usage of ECC in wireless devices is more superior to public key encryption techniques. Once **V.Gampala, S. Inuganti, S.Muppidi [2]** as talk about the "Modified RSA Encryption Algorithm (MREA)" where they talk about use of factorization method in RSA cryptosystem, and its implementation comparing the existing system and their system with key sizes up to 1024 bit. Elliptic Curve Cryptography is a secure and more efficient encryption algorithm than RSA as it uses minor key sizes for equal level of security as compared to RSA. For e.g. a 256-bit ECC public key provides differentiate security to a 3072-bit RSA public key. The aim of this work is given by insight into the use of ECC algorithm for data encryption before uploading the data on to the cloud.

III. PROPOSED SYSTEM

Design will elaborate the process of describing, organizing and structuring the components of the system both at the architectural level and at the detailed level.

The block diagram shows that admin logins to system can select a file encrypts the file using ecc algorithm. Admin uploads the file into cloud.

The block diagram shows that admin logins to system can select a file encrypts the file using ecc algorithm. Admin uploads the file into cloud.

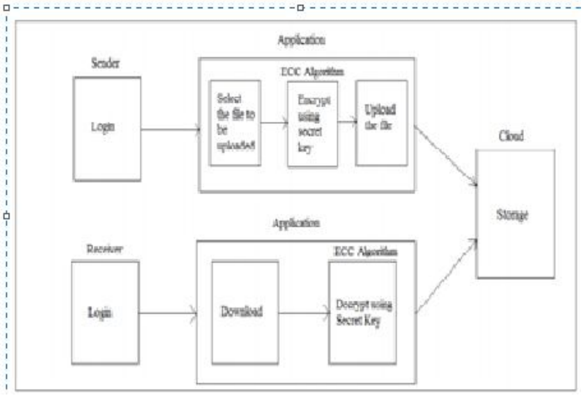


Fig 1:Block Diagram Of Proposed System

ELLIPTICAL CURVE CRYPTOGRAPHY ALGORITHM

Elliptic Curve cryptography (ECC) is cryptographic plan that uses the properties of elliptic curve to create cryptographic calculations. In the 1980s Koblitz and Miller proposed utilizing the gathering focuses on elliptic curve cryptography. Over a limited field in discrete logarithmic cryptosystems. An elliptic curve is the arrangement set over a non particular cubic polynomial mathematical statement with two questions over a field F. In short terms it is a discretized set of answers for a curve that is in the structure:

$$y2 = x3 + ax + b$$

If P1 and P2 are points which on the curve E,

$$P3 = P1 + P2$$

Both clients consents to some publicly aware of information items.

1. The elliptic curve mathematical statement
2. Estimation of a and b
3. prime, p
4. The elliptical curve figure gathered from the elliptic curve equation
5. A base point, B, taken from the elliptic gathering.

Key generation:

1. A choose a whole number dA. this is A‘s private key. 2. A then produce a public key PA= dA*B
2. B correspondingly chooses a private key dB and process an public key PB= dB *B
3. A produces a security key K= dA *PB. B produces the security key K= dB *PA.

Signature Generation:

For marking a message m by A, utilizing A‘s private key dA

1. Compute e=HASH (m), where HASH means cryptographic hash function, such as SHA-1
2. Select a arbitrary whole number k from [1, n − 1]
3. Compute r=x1(mod n), where(x1, y1) =k*B. If r=0, go to step 2
4. Computes=k−1(e+dAr)(mod n).Ifs=0,gotostep2
5. The signature is the couple of (r, s).
6. Send signature (r, s) to B client.

Encryption algorithm:

Suppose A wants to send to B an encrypted message.

1. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic gathering.
2. A picks another arbitrary whole number, k from the interval [1, p-1]
3. The cipher text is a couple of points.
4. PC = [(kB), (PM + kPB)]
5. Send cipher text PC to client B.

Decryption algorithm:

Client B will take the following steps to decrypt cipher text PC.

1. B computes the result of the principal point from PC and his private key, dB dB * (kB)
2. B then takes this item and subtracts it from the secondpoint from PC
3. (PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM
4. B cloud then deciphers PM to get the message, M.

Signature Verification:

For B to authenticate A's signature, B must have A‘s public key PA

Confirm that r and s are whole numbers in

1. [1, n − 1]. If not, the signature is invalid.
2. Evaluate e = HASH (m), where HASH is the same function used in the signature generation.
3. Evaluate w = s −1 (mod n)
4. Evaluate u1 = ew (mod n) and u2 = rw (mod n)
5. Evaluate (x1, y1) = u1B + u2PA
6. The signature is valid if x1 = r (mod n), invalid otherwise.

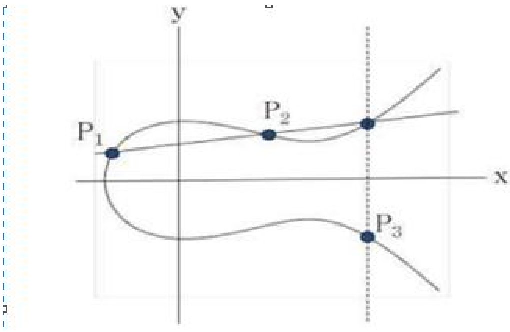


Fig 2:ECC Algorithm

As shown in figure. Let P1=(x1, y1), P2=(x2, y2), P3=(x3,y3) and P1 not equals P2.

$$m = \frac{y_2 - y_1}{x_{2} - x_1}$$

To find the insertion with E. we get

$\left(m(x - x_1) + y_1\right)^2 = x^3 + Ax + B$

Or, $0 = x^3 - m^2 x^2 + \cdots$

So, $x_3 = m^2 - x_1 - x_2$

$y_3 = m(x_1 - x_2) - y_1$

IV. RESULTS

Short key size: ECC produce comparatively short encryption key, this key value that must be given to the encryption algorithm ignored to decode an encrypted message. The short key is much faster and its require very less computing power than many other algorithms. For example, a 160-bit ECC encryption key algorithm provides the same security as that of 1024-bit RSA encryption key algorithm and which is up to 15 times faster, generally its depend on the platform on which it is implemented.

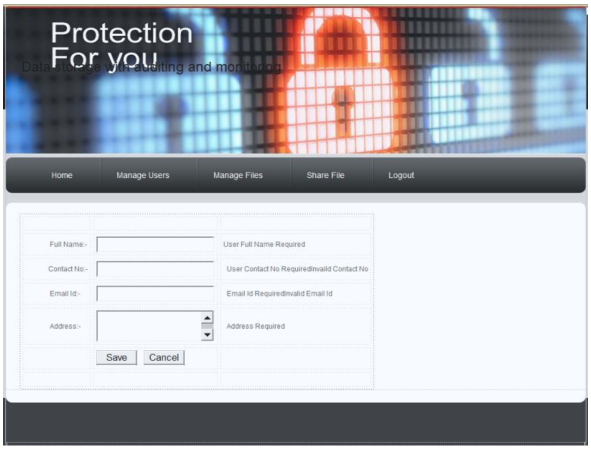
Power Consumption: ECC requires comparatively very less power for its functioning hence it is more applicable for low power applications such as handheld and mobile devices.

Computational Efficiency: Implementing scalar multiplication in software and hardware is much more feasible than performing multiplications or exponentiations in them. As ECC makes use of scalar multiplications, so it is much more computationally efficient than RSA

LOGIN PAGE

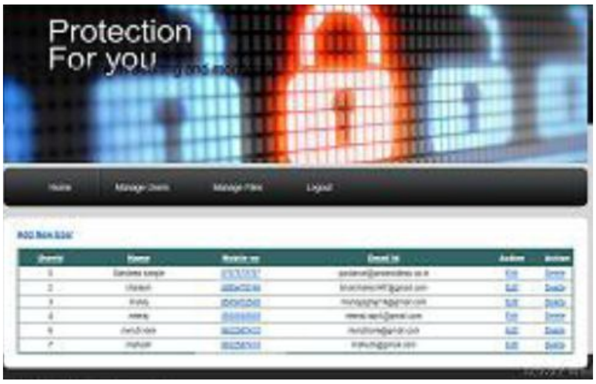
HOME PAGE

ADMIN: ADD NEW USER PAGE



Full Name:-		User Full Name Required
Contact No:-		User Contact No RequiredInvaild Contact No
Email Id:-		Email Id RequiredInvalid Email Id
Address:-		Address Required

MANAGE USER PAGE



[illegible]	Name	Mobile no	Email Id	Action	Action
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete
[illegible]	[illegible]	[illegible]	[illegible]	Edit	Delete

V. 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.

REFERENCES

[1] R. Gharshi, Suresh, “International Journal of Science and Research (IJSR)”, Volume 2 Issue 7, July 2013,pg no 56-64, India Online ISSN: 2319-7064.

[2] V.Gampala, S. Inuganti, S.Muppidi,” Data Security in Cloud Computing with Elliptic Curve Cryptography ”, International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-3, July 2012,pg no 131-134, ISSN: 2231-2307.

[3] S.Alshehri, S.Radziszowski, R.K. Raj,” Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption.”, Golisano College of Computing & Information Sciences.Rochester Institute of Technology,Rochester, New York 14623, USA.sxa3788@rit.edu, spr@cs.rit.edu, rkr@cs.rit.edu, pg no 1-5.

[4] IBM, “Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges,” http://www-03.ibm.com/press/us/en/pressrelease/22414.wss.

[5] http://en.wikipedia.org/wiki/Cloud_computig

[6] http://www.cloudcomputingchina.cn/Article/luilan/200909/306.html

[7] http://searchcloudcomputing.techtarget.com/s Definition/0,,sid201_gci1287881,00.html

[8] http://www.boingboing.net/2009/09/02/cloud-computing-skep.html