International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

Secure Data Storage on Cloud System for Privacy Preserving

Kshitija Pendhari[1], Ashwini Pawar[2], Aishwarya Erunkar[3] , Ankush Hutke[4]

[1]*Student VIII SEM, B.E., Information Technology. , RGIT, Mumbai, India*
[2]*Student VIII SEM, B.E., Information Technology. , RGIT, Mumbai, India*
[3] *Student VIII SEM, B.E., Information Technology. , RGIT, Mumbai, India*
[4] *Professor, Department of IT, RGIT, Mumbai, India*

Abstract - *Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy with necessary regulations. The main aim of the system which customers can take care of is to encrypt their data before it is stored on the cloud. The goal of the system is intended towards providing security service such as confidentiality in the cloud services can use Elliptic Curve Cryptography (ECC) algorithm and Shamir's Secret sharing algorithm.*

Key Words: **Data Security, Cloud Technology, Elliptic Curve Cryptography (ECC), Shamir Secret key**

1. INTRODUCTION

Cloud is a model where users have a convenient, on- demand access to a shared pool of resources, such as servers, storage, and applications, over the Internet. Cloud computing is a type of internet-based computing that provides shared computer processing resources and data to computers. The entire process of requesting and receiving resources is automated and is completed in minutes by just sharing the keys with the authenticated users.The cloud storage is fulfilling the need for large 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.

As shown in Figure 1, cloud storage can be used from smaller computing devices to desktop computers and servers.

Figure 1: Cloud storage

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.

1.1 Existing Technology

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978.
RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private.
RSA algorithm is the first generation algorithm that was used for providing data security. It can be used to encrypt a message without the need to exchange a secret key separately. Its security is based on the difficulty of factoring large integers.

1.2 ECC Algorithm

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

Assume that those who are going through this article will have a basic understanding of cryptography (terms like encryption and decryption) .

The equation of an elliptic curve is given as,

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

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

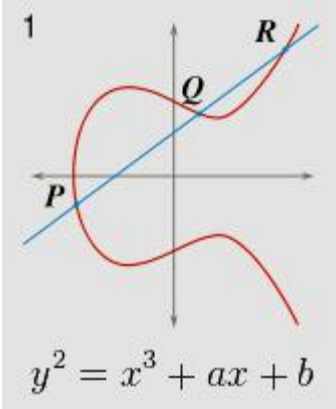

Figure 2: Simple Elliptic Curve

The Figure 2 shows simple elliptic curve.

Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number **'d'** within the range of **'n'**.

Using the following equation we can generate the public key

Q = d * P

d = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

'Q' is the public key and **'d' is the private key.**

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. This have in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Conside 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that we have send.

Proof

How does we get back the message,

M = C2 – d * C1

'M' can be represented as 'C2 – d * C1'

C2 – d * C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

ECC(in bits)	RSA(in bits)
106	512
112	768
132	1024
160	2048
210	3072
283	7680
409	15360
571	21000

Table 1:Key Size Of ECC and RSA

Table 1 describes key size of RSA algorithm and Elliptic Curve Cryptography (in bits) which described one of protocol as ECDSA.

Advantages of ECC over RSA

- Low on CPU consumption.
- Low on memory usage.
- Good protocols for authenticated key exchange
- Moderately fast encryption and decryption.
- Smaller keys, cipher texts and signatures.
- Very fast key generation.

2. LITERATURE REVIEW

[1] Cong Wang, Qian Wang, KuiRen, Wenjing Lou
Cloud computing enables companies to consume a compute resource, such as a virtual machine (VMs), storage or an application, as a utility -- just like electricity -- rather than having to build and maintain computing infrastructures in house.Cloud computing may not be fully trustworthy as it moves the application software and databases to the large data centers where the management of the data and services takes place.

[2] B.Banu priya, V.Sobhana, Prof.Mishmala Sushith
It is a concise survey on various privacy preserving techniques in cloud. Homomorphic Authenticable Ring Signature (HARS), privacy-preserving public auditing System for data storage security. Public key cryptosystem, the MD5 Message-Digest Algorithm are used. Proof-Of-Retrievability system for public verifiability is described. Dynamic Provable Data Possession (DPDP) to enlarge the PDP model is discussed in detail.

[3] R. Rajasaranyakumari, S.Velmurugan, K.J. Nithya Cloud is used not only for storing large amount of data, but also the stored data that can be shared by multiple users. Due to this the integrity of cloud data is insecure. There are several mechanisms designed to support public auditing on shared data stored in the cloud. During auditing, the shared data is kept private from public verifiers, who are able to verify shared data integrity using ring signature without downloading or retrieving the entire file. Ring signature is used to compute verification metadata needed to audit the correctness of shared data.

[4] Boyang Wang, Baochun Li, and Hui Li
First privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

3. SYSTEM ANALYSIS

A. Problem Definition

There are many secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption, the best solution is to combine public and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. Public-key cryptography may be vulnerable to impersonation, even if users' private keys are not available.

B. Proposed System

Our proposed system can be enhanced by providing effective security by using Shamir's secret sharing algorithm and ECC algorithm. It also provides fast service to store data on server. It also gives proof of integrity of the data to client. This scheme reduce storage overhead of the customer by compressing the data and reduce computational overhead of the cloud storage server.

User can share their data using cloud. The data will be shared using Elliptic Curve Cryptography (ECC) algorithm and Shamir's Secret Sharing Algorithm. The user will upload the data in cloud, the data will be encrypted using Elliptic Curve Cryptography (ECC) algorithm, provided that some set of keys will be generated and it will be mailed to the user. User get the mail which contains key for decryption and share keys for authentication.
The generated Shamir keys are like 'qlMckNy3' , '25DrYCKN', 'D1SMq2Ie' ,'WAZBod2y' , 'deof8tmZ' ,'5du9mzUk' ←This is the mail content. User can share these keys to the another user with whom he wants to share his data.The person at receiver side enters the keys and if the keys are matched then only he can access the data.

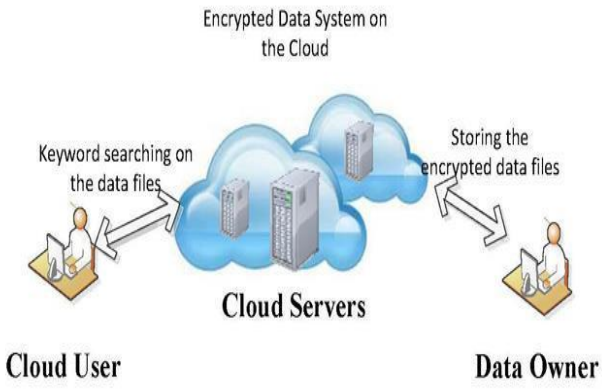

Figure 3:Workflow of the system
The Figure 3 represents the workflow of the system.

C. System Module

- **Sender Login**:- In this module sender login into the system using username and password. If username and password matches then sender get access to the application.
- **Encryption Module**:- In the module sender uploads the data then the data is 1st encrypted using ***Elliptic Curve Cryptography*** ,and the keys are generated and it is send to the receiver. The Receiver encrypt the data using ***Shamir secret***

- ***sharing algorithm .***
- **Receiver Login**:- In this module receiver login into the system using username and password. If username and password matches then receiver get access to the application.
- **Decryption Module**:-Receiver decrypt the data using the set of Shamir keys provided by the sender to the receiver.
- **Signature Verification Module**:-Receiver keys are verified with the senders keys ,if the keys are matched then receiver can access the data else not.

4. CONCLUSIONS

The secure data on cloud system for privacy preserving. We utilize the ECC algorithm for encryption and decryption, so that admin is able to audit the integrity of shared data. The ECC has many advantages due to its ability to provide the same level of security as RSA yet using shorter keys. However, its disadvantage which may even hide its attractiveness is its lack of maturity, as mathematicians believed that enough research has not yet been done in ECC. We further extend the mechanism of Shamir's secret key for key generation which provides authentication to client.

5.REFERENCES

[1] "C. Wang, Q. Wang, K. Ren, and W. Lou", "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *in Proc. IEEE INFOCOM, 2010, pp. 525–533*

[2] "B.Banu priya, V.Sobhana, Prof.Mishmala Sushith", "Provable Data Possession at Untrusted Stores," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 598–610.

[3] "R. Rajasaranyakumari, S.Velmurugan, K.J. Nithya", Enhanced Privacy Preserving with Data Freshness by *Accomplishing Traceability over Oruta, IJRASET,October 2014*

[4] "Wang, Baochun Li, and Hui Li ","Privacy- Preserving Public Auditing for Data Storage Security in Cloud", Co"Boyang mputing,"in Proc. IEEE International Conference on Computer Communications(INFOCOM), 2010, pp. 525–533

[5] https://bithin.wordpress.com/2012/02/22/simple-explanation-for-elliptic-curve-cryptography-ecc/