Application of Elliptical Curve Cryptography in Empowering Cloud Data Security

T. Venkat Narayana Rao[1]
Professor, Dept. of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

Vanaparthy Sai Praneeth[2]
Student, Dept. of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India

K. Sai Sharath [3]
Student, Dept. of Computer Science and Engineering
Sreenidhi Institute of Science and Technology
Hyderabad, India.

Abstract: Cloud computing is one of the most preferable and used technologies in IT Industry in the present scenario. Providing security to cloud data in cloud environment has become popular feature in industry and academic research. Cloud Computing is a conceptual concept based on technology that is widely used by many companies these days. The Elliptical Curve Cryptography algorithm ensures the integrity and authentication of secure communications with non-repudiation of communication and data confidentiality. Elliptical Curve Cryptography is also known as a public key cryptography technique based on the elliptic curve theory that can be used to create a fast, small, more efficient and unpredictable cryptographic key. This paper provides authentication and confidentiality to cloud data using Elliptical Curve Cryptography. This paper attempts to evolve cloud security and cloud data security by creating digital signatures and encryption with elliptical curve cryptography. The proposed method is an attempt to provide security to encryption keys using access control list, wherein it lists all the authorized users to give access to the encryption keys stored in cloud.

Keywords*: Cloud Computing, Data security, Cloud security, Encryption, Decryption, Elliptical Curve Cryptography, Digital signature, Elliptic Curve Theory.*

*****

I. INTRODUCTION

Cloud is basically a combination of servers at very high level. Cloud computing allows us to access the internet applications and services over internet. It allows us to create, configure and customize online applications. Cloud computing refers to accessing and making use of the hardware and software resources remotely. It provides online data storage of data. Cloud computing enables executing application directly on the cloud without being application to be installed on the local machine as shown in figure 1. This paper focus on the data security and cloud protection inside the cloud processing that can be attained by the application of cryptographic algorithms.

Fig 1: Cloud Computing

A. CRYPTOGRAPHY

Cryptography is the discipline or art of changing the text to an encoded form that makes text ineligible for those who need not read. This process of plaintext conversion using a mechanism known as encryption. Decryption is to re-conversion of cipher text back plaintext. In a private key cryptography process, the encryption and decryption are performed using a alike key which is secret key. The popular examples are AES and DES algorithms. Public key cryptography is also called as asymmetric key cryptographic systems. A key is basically a value used in a cryptography algorithm to translate raw text to cipher text. This has great value and is measured in several parts. It is observed that the more the key size used in the public key cryptography, the more the secure the cryptographic mechanism would be.

B. DATA SECURITY

To produce data, most systems employ a combination of methods, that includes:

1. Encryption means using a complex expression to encode the data. In order to decode the encrypted data files, a user requires an encryption key. While a user can obtain a cipher text but it is in illegible format in order to decrypt the cipher text any user

needs a key , unauthorized users are prevented to access the encryption key to offer security to private data.

2. Authentication procedure deal with creation of a user name and security password.

3. Authorization practices - the cloud service providers(CSP) enlist the users who are authorized to access information placed on the cloud server. To secure user information every time on different application diverse cryptographic algorithms and authentication procedures are employed. Due to small processor speed and run time memory; the devices require an algorithm which can be utilized in small computer devices also. Security of stored data and data in transition might be a concern while storing sensitive data on the cloud storage.

C. CLOUD SECURITY ISSUES

There are 3 basic problems with cloud computing safety , that are: confidentiality, integrity and availability as shown in figure 2.

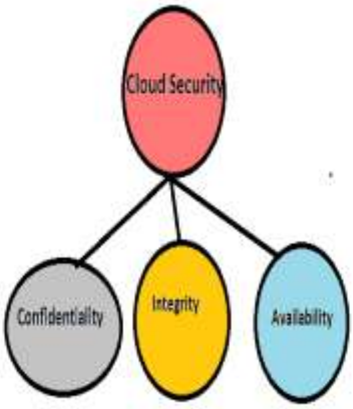


Fig 2: Cloud Security Issues

Confidentiality: Confidentiality refers to authenticated person would be able to access and retrieve the data. So in order to protect the confidentiality of information, the information is encrypted by the authorized person and later be able to decrypt it as the information as key being known to him only. There are two main threats of confidentiality those are snooping and traffic analysis. Other ways to ensure information confidentiality include enforcing file permissions and access control list to restrict the access to sensitive information[4][8].

Integrity: Integrity is a act of protecting information from being modified by unauthorized parties. This is a commonly used method to protect data integrity which includes hashing the data received and comparing it with the hash of the initial/original message. However, this means that the hash of the original data must be provided in a secure fashion. More convenient methods could be to use existing schemes such as GPG to digitally sign the data.

Availability: Availability is the information that is needed to the authorized user whenever needed. There is need to worry about confidentiality and integrity if the approved users cannot get the information they are entitled to. It is one of the most important feature of information security.

II. Basic Concepts and Literature

This paper provides an overview of the security issues of data protection and privacy associated with cloud computing. The methods presented in this study focus on enhancing security in cloud computing and privacy protection by offering digital signature generation and verification , encryption and decryption mechanisms[1]. This approach offers cloud and data security by providing protection to keys that are employed in encryption and decryption. It is the combination of digital signature algorithm of Diffie Hellman and Elliptical Curve Cryptography encryption [4]. This method can be used to prevent any unauthorized access to the privately data stored on the cloud by any user. It is noticeable that usage of Elliptical Curve Cryptography in wireless devices is superior to public key encryption techniques. It aids in minimizing the processing time of the devices[1][2].

The existing system uses Elliptical Curve Cryptography algorithm for provisioning security to user's data but it do have some limitations in terms of key distribution and number of keys shared under different attacks. In the existing system private key is stored by partitioning private key into 3 different parts and this is stored on three different storage locations, hence, there is huge possibility that the hackers might perform several attacks to access authenticated user's data that is stored on diverse locations in the cloud[2]. All these processes are shown in existing model i.e. in figure 3.

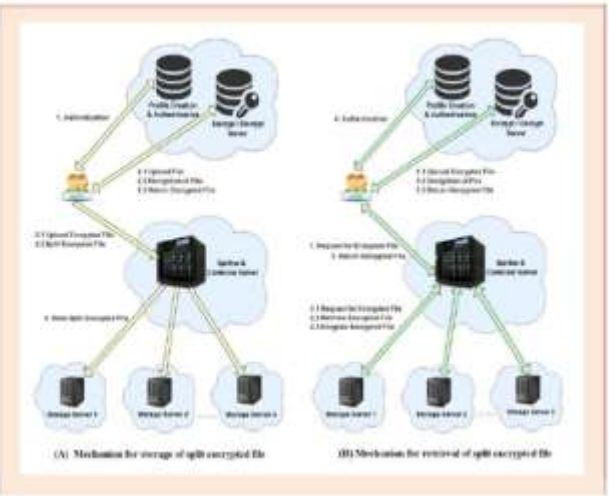


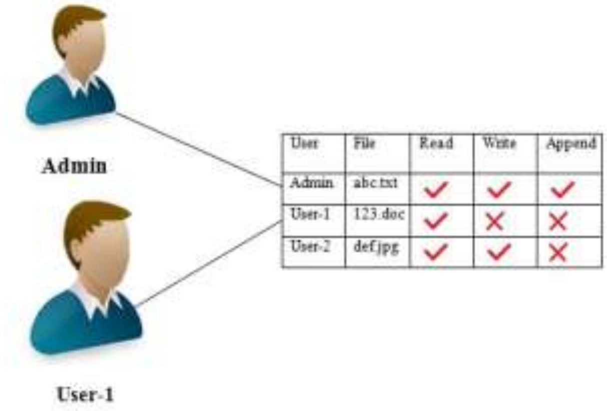
Fig 3: Existing Model of security

III. Implementation and Evaluation

In the proposed system the digital signature is utilized for authentication and AES algorithm is employed for encryption in order to make the data safe in cloud environment [5][6].

Storing data and security of data is the major liability of the cloud provider. Hence, for competent data security and consistency a mechanism is needed which offers secured data encryption and decryption to provide a shield against the theft and attacker. So, this system is implemented to provide improved cloud data security in cloud computing using Elliptical Curve Cryptography that provides additionally security on data transmission, storage, authorization, and authentication processes [6][7].

In the existing system, private data is encrypted using encryption keys, and the encryption keys are partitioned into numerous parts and are stored in dissimilar locations of cloud. Hackers can perform many attacks and acquire the access of encryption keys stored in various locations of cloud database. In the proposed system in order to enhance the security in the cloud data storage an attempt is made to keep a lock on the encryption key from illegal access. An access control list is arranged for the encryption key so that only permitted users nominated in the access control list can obtain the access to the encryption keys used for encryption and decryption of private data stored in cloud. Encryption key is safe guarded by a lock, whenever an user need to access key, validation occurs and checks in the access control list to ascertain the user eligibility to access the key stored in the cloud database. If the user is found to be appropriate then only access the key, lock is released on a particular key, upon conclusion the key is yet again protected by the lock as shown in figure 4.



User	File	Read	Write	Append
Admin	abc.txt	✓	✓	✓
User-1	123.doc	✓	✗	✗
User-2	def.jpg	✓	✓	✗

Figure 4: Proposed Control Access List Model

The Elliptical Curve Cryptography

Elliptic Curve cryptography (ECC) is a cryptographic scheme that employs the features of elliptic curve to produce cryptographic calculations[3][5]. In 1980s Koblitz and Miller had proposed the elliptic curve cryptography. Over a restricted field in discrete logarithmic cryptosystems , an elliptic curve is the arrangement over a non-particular cubic polynomial mathematical statement with two questions over a field F.

In short terms it is discretized set of outcomes for a curve that is in the following structure:

y2 = x3 + ax + b (1)

If points P1 and P2 lie on the curve E, P3 = P1 + P2. Assume both the clients follow a mathematical statement as given here under in the pseudo-code :

1. The elliptic curve mathematical statement
2. Estimation of values a and b
3. Assume a prime number , p
4. The elliptical curve figure is produced from elliptic curve equation
5. A base point, B is drawn from the elliptic gathering.

Key generation process:
1. UserA chooses a whole number dA i.e. UserA‘s private key.
2. UserA generates public key PA= dA*B
3. UserB correspondingly selects a private key dB and compute public key PB= dB *B
4. UserA generates a security key K= dA *PB. UserB produces the security key i.e. K= dB *PA.

Signature Generation: For marking a message m by UserA, use UserA‘s private key dA :

1. Compute e=HASH (m), wherein, HASH means cryptographic hash function, such as SHA-1
2. Opt for an arbitrary whole number k from the range [1, n − 1]
3. Calculate r=x1(mod n), where (x1, y1) =k*B and If r=0, Then go to step 2
4. Computes k−1(e+dAr)(mod n).If s=0, then go to step2
5. The signature is a couple as (r, s).
6. Send signature (r, s) to client UserB.

The Encryption algorithm: Suppose UserA intends to transmit encrypted message UserB.
1. UserA takes plaintext message M, and encodes it onto a point, PM, from the elliptic gathering.
2. UserA picks another arbitrary whole number, k from the interval ranging [1, p-1]
3. The cipher text is a couple of points i.e.
PC = [(kB), (PM + kPB)]
5. Send cipher text PC to UserB.

The Decryption algorithm: UserB assumes following steps to decrypt the cipher text PC.
1. UserB computes the result of the main point from PC and his private key i.e. dB dB * (kB)
2. UserB then takes this data item and subtracts it from the second point from PC
3. (PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM
4. UserB might deciphers PM to get the originalmessage, M.

Signature Verification: Inm a process for UserB client to authenticate UserA's signature, UserB must have UserA‘s public key PA

1. Confirm that r and s values are whole numbers in the range of [1, n − 1]. If not, the signature is invalid.
2. Evaluate value e = HASH (m), wherein HASH is the same function utilized in the signature generation.
3. Evaluate value w = s −1 (mod n)
4. calculate u1 = ew (mod n) and u2 = rw (mod n)
5. calculate (x1, y1) = u1B + u2PA
6. The signature is valid if the value of x1 = r (mod n), otherwise invalid.

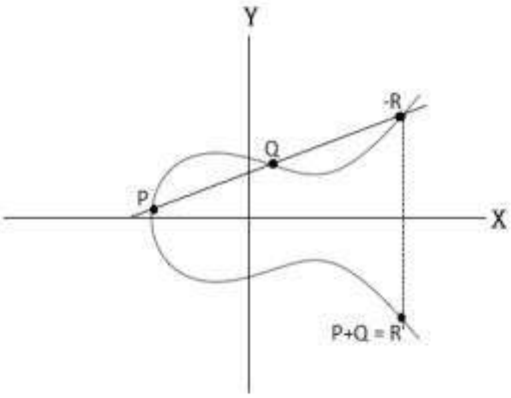


Fig 5:Elliptic Curve

As shown in the above figure 5, 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 the insertion with E. we get

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

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

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

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

Point Addition:

- R=P+Q
- S=(Py-Qy)/(Px-Qx)
- Rx=S^2-Px-Qx
  - Ry=S*(Px-Rx)-Py

Example:

P=(-2.35, -1.86)

Q=(-0.10, 0.836)

–R(3.89, 5.62) and R(3.89, -5.62)

P+Q=R=(3.890, -5.620)

Point Doubling:

1.R=2.P

2.S=(3*Px^2+a)/(2*Py)

3.Rx=S^2 -2*Px

4.Ry=S*(Px-Rx)-Py

For Example:

P(2, 2.65),

–R(-1.11, -2.64),

R(-1.11, 2.64)

2P=R=(-1.11, -2.64)

For Example:

UserA Encrypts:

1 .Suppose UseA wants to send a message to UserB.

2. Plaintext is x=(10,9) which is a point in E

3. Select a random value for k, k=3

4. Now compute (y1,y2):

y1=3(2.0,7.00)=(8.00,3.00)

y2=(10,9)+3(7,2)

=(10,9)+(3,5)

=(10.0,2.00)

5. UserA transmits y=((8,3),(10,2))

UserB Decrypts:

1.UserB receives y=((8,3),(10,2))

2.Compute x=(10,2)-7(8,3)

=(10,2)-(3,5)

=(10,2)+(3,6)

=(10,9)

(10,9) which is the plaintext. In this way UserB is able to find original message (10,9) which is delivered by UserA to UserB.

Application of ECC

Many devices are small and have limited storage and computational power. Following are the key devices used in the present scenario.

1.**Wireless communication devices**

2. Smart digital cards

3.Web servers that need to handle many encryption sessions. Any application that need security usually lacks in power, storage and computational power which happens to be very much necessary for the current cryptosystems.

IV. Conclusion and Future Work

Elliptic Curve Cryptography provides better security and has shown efficient performance compared to first generation public key cryptography techniques like RSA which is now in use. After comparing the RSA and ECC ciphers, the ECC has manifested a feature to withstand complex scenarios and has exhibited less overheads as compared to RSA. The ECC has many merits due to its ability to provide the same level of security using less key size. ECC is suitable for many devices that are small and have limited storage and computational power to implement encryption and decryption on private data. The future of ECC looks brighter than other algorithms as today’s applications include smart cards, pagers, and cell phones and do not witness overheads introduced by RSA algorithm. Although ECC’s security has not been completely evaluated, it is expected to come into widespread use in diverse fields in the future. Before introducing ECC onto larger networks, it must be thoroughly tested to improve the security and efficiency i.e in terms of application to application.

REFERENCES

[1] Deyen Chen Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing, Computer Science and Electronics Engineering (ICCSE), 2012 International Conference on (Vol.:1) ePrint-23-25 Mar.2012.

[2] Ramgovind, S. Eloff, M. ; Smith, E, The management of security of Cloud computing, Information Security for South Africa (ISSA), 2010, ePrint 2/4August.

[3] Parsi Kalpana , Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication tech., IJRCCT, Sept. 2012.

[4] Neha Tirthani, and Ganesan.R R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, International Association for Cryptologic Research Cryptology vol. 4-9, 2014.

[5] Prof Swarnalata Bolavarapu, Bharat Gupta, Data Security in Cloud Computing, Int’l Journal of Advanced Research in Computer Science and Software Engineering , Vol.4/ 3, March 2014.

[6] Dhaval Patel, M.B.Chaudhri, Data Security In Cloud Computing Using Digital Signature, International Journal For Technological Research In Engineering , June-2014.

[7] N. Koblitz, elliptic curve cryptosystem, Mathematics of Computation, Vol. 48-1987, PP-203-209.

[8] Ms. Bhavana Sharma, Security Architecture Of Cloud Computing Based On Elliptic Curve Cryptography (ECC), International Journal of Advances in Engineering Sciences Vol.3/3, July, 2013.

[9] Ms. Priyanka Shaarda, Providing data security in cloud computing using elliptical curve cryptography, Int’l Journal on Recent and innovation trends in computing and communication, volume3/2, 2015.