IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

Enhancing Cloud Data Security Using Elliptical Curve Cryptography

Ms. Nikita N Chintawar[1], Ms. Sonali J Gajare[2], Ms. Shruti V Fatak[3], Ms. Sayali S Shinde[4], Prof. Gauri Virkar[5]

Bachelor of Engineering, Information Technology, BSIOTR, Pune, India [1, 2, 3, 4]

Professor, Computer Science and Engineering, BSIOTR, Pune, India[5]

Abstract: Cloud computing is one of the hottest technology of the IT trade for business. Cloud computing security has changed into a popular topic in sector and academic research. Cloud Computing is a conceptual service based technology which is used by many companies widely these days. ECC algorithm provides secure communication integrity and authentication, along with non_repudiation of communication and data confidentiality. ECC is known as a public key encryption technique based of Elliptical Curve theory that can be used to create speedy, tiny and more efficient cryptography key. It has three protection points: authentication, key generation and encryption of data. This paper will create cloud security and data security of cloud in cloud computing by creating digital signature and encryption with elliptical curve cryptography.

Keywords: Cloud computing, Data security, Cloud security, Encryption, Decryption, Elliptical Curve Cryptography, Digital signature.

I. INTRODUCTION

Cloud is basically a combination of servers at very high level. The combination of servers is virtually said to be in space, so it is called as cloud. Cloud computing is a term that involve to deliver the services over the Internet. Cloud computing allows computer users to conveniently rent access to fully featured applications, to software development and deployment environment, also to processing infrastructure assets such as network-accessible storage data and processing. Cloud computing can be a model for enabling convenient, on-demand network access to a shared pool of configurable computing assets. In this paper we certainly have discussed about the data security and cloud protection inside the cloud processing that can be attend by applying the cryptographic algorithms.

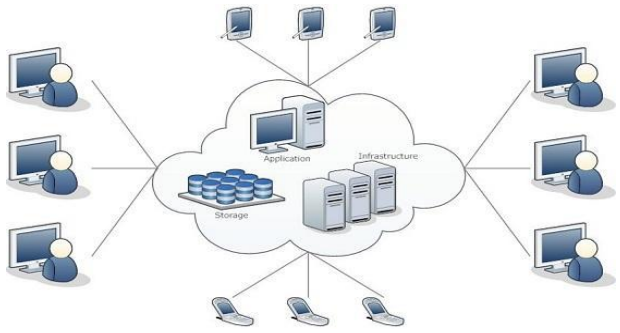

Fig 1: Cloud Computing

A. CRYPTOGRAPHY

Cryptography is the science or art of changing text to a coded form that makes the text unreadable for those people you don't want to read it. The process of converting plain text tocipher text using some mechanism is called encryption. Decryption is converting the cipher text back to simple text form. In private key cryptography, the encryption and decryption both happen to be done using the same key. Examples are AES and DES. Public key cryptography is also known as asymmetric key cryptography. A key is basically a value that is used in an algorithm for cryptography to convert plain text to cipher text. That has a huge worth and is also measured in parts. The larger the key is usually in public key element cryptography, the more secure is the cryptographic mechanism.

B. DATA SECURITY

To generate data, most systems make use of a combination of techniques, which includes:

1. Encryption means using a complex formula to encode information. To decode the encrypted data files, a user needs an encryption key. While it is possible to crack protected information, most hackers have no access to the sum of computer processing power that they would need to decrypt information.

2. Authentication procedures, which require creating a great user name and security password.

3. Authorization practices -- the customer lists the persons who are authorized to access information placed on the cloud system.

To secure user data almost all of times used different cryptographic algorithm and authentication procedure in which passwords are used. Due to smaller processor speed and run time memory; these devices need an algorithm which can be utilized in such small computer devices. Security of stored data and data in transit may be a concern while storing sensitive data at a cloud storage provider.

C. CLOUD SECURITY ISSUES

The three problems with cloud computing safety are: confidentiality, integrity and availability; shown in figure.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

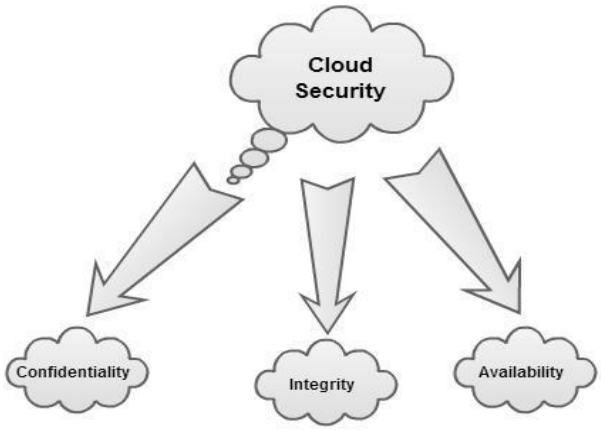

Fig 2: Cloud Security issues

Confidentiality:
Confidentiality means only the authenticated person should be able to access and retrieve the data. So in order to preserve the confidentiality of information, the information is encrypted with only the authorized person and he being able to decrypt it because of some information known only to him. 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 access to sensitive information.

Integrity:
Integrity means to protect information from being modified by unauthorized parties. Commonly used methods to protect data integrity include hashing the data you receive and comparing it with the hash of the original message. However, this means that the hash of the original data must be provided to you in a secure fashion. More convenient methods would be to use existing schemes such as GPG to digitally sign the data.

Availability:
Availability is the part that guarantees the individuals which have the rights to access the information i.e. information is available to user when it is needed. There is no use of confidentiality and integrity if the approved users cannot get the information they are entitled to. It is one of the most important characteristics.

II. LITERATURE SURVEY

This paper provides an overview of different data security and privacy protection issues associated to cloud computing. This method focuses on ensuring security in cloud computing and privacy protection by giving secured honest cloud computing environment [1]. This paper discussed about management of security issues concerned with cloud computing, some serious security threats that prevails this field and management of the threads and attacks [2]. RSA system for data security is proposed in this paper. The RSA algorithm is used for encrypting large files and storing the data. The system can be used for storing big databases but it is handled by linear methods compromises with the data fetching speed. Hence, this system is excellent way for static data [3]. In this paper proposed a system to provide a cloud security and data security. It is the combination of digital signature algorithm of Diffie Hellman and ECC encryption [4]. ECC, RSA, RC4 and El-Gamal algorithms are adviced and mentioned for cloud computing in this paper. 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. It helps in longer the lifetime of batteries of the devices [5]. Proposes a system for providing security to user information in cloud computing using digital signature generation and verification. In proposed system use the digital signature for authentication and AES as encryption algorithms for data safety measures in cloud computing [6].

III.EXISTING SYSTEM

RSA algorithm is used in the existing system for encryption and decryption process. RSA algorithm is the most widely used public key cryptography algorithm for encryption and decryption by many vendors today. The RSA algorithm can be used for both public key encryption and digital signatures. RSA is also known as asymmetric key encryption and decryption algorithm used in cryptography which uses two keys for both encryption and decryption process. The key is known as the public key which has been send to the sender and receiver. Sender while sending the information to the receiver along with the encryption of the information using his public key. The receiver can decrypt the data with his private key. With the help of the private key again the decrypted text has been converted into plaintext which is the actual text in readable format. RSA can also be used to sign a message, so A can sign a data applying their private key and B can check it using A's public key. In the existing system used ECC Algorithm. ECC is an asymmetric key cryptography system which is used for encryption and decryption of user data. This cryptosystem uses the different keys for encryption and decryption process. There are two keys public and private, using public key A can be encrypt the all data before it send to the B along with digital signature which is in xml format and firstly B can verify this digital signature for authentication purpose and then decrypt the data using his private key. But drawback of this system is that, if an adversary is successful in inferring the private key of an authenticated user which is stored on database server using different attacks then the privacy of the authenticated user may be in danger. Hence, there is a need to provide more security to the private key of the authenticated user.

A. Advantages of Existing System:
1. Smaller keys are as robust as larger key for RSA.
2. Cheap CPU consumption.
3. Memory usage is low.
4. Size of encrypted data is smaller.

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

DOI 10.17148/IJARCCE.2016.5327

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

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.

B. Disadvantages of Existing System:

1. Hyper elliptic cryptosystems offer even smaller key sizes.
2. ECC increases the size of the encrypted message significantly more than RSA encryption.
3. ECC is mathematically more subtle than RSA.
4. Difficult to explain/justify to the client, more complex thereby reducing the security of the algorithm.

IV. PROBLEM STATEMENT

Storing of user data and security of that data is main responsibility of the cloud provider. So, for efficient data security and reliability we need mechanism which provides secure data encryption, decryption as well as secure shield against the theft and attacker. Many problems like Data Security, Cloud Security issues and different cryptographic algorithms are discussed in literature review. So, this system implement to provide better cloud data security in cloud computing using Elliptical Curve Cryptography which gives more secure data transmission, storage, authorization, and authentication process over the cloud.

V. PROPOSED SYSTEM

The existing system prefer ECC algorithm for provisioning security to user's data but the main limitation of this system is that it is not hard to an adversary to infer the private key using different attacks. Hence, in the proposed model attempt is made to provide more security to authenticated user's data and private key by partitioning private key into three different parts and this stored on three different storage locations. Due to this approach it becomes for an attacker to infer the original private key. Hence, compared to existing system proposed system provide better security. All this process shows in given proposed model.

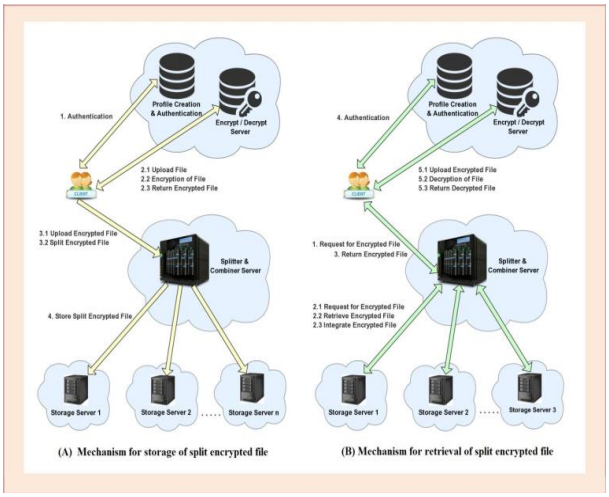

Fig 3: Proposed Model

A. Elliptical Curve Cryptography

Elliptic Curve cryptography (ECC) is a 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:

$$y2 = x3 + ax + b \text{---------- (1)}$$

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
3. B correspondingly chooses a private key dB and process an public key PB= dB *B
4. 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 second

DOI 10.17148/IJARCCE.2016.5327

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

point 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

1. Confirm that r and s are whole numbers in [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.

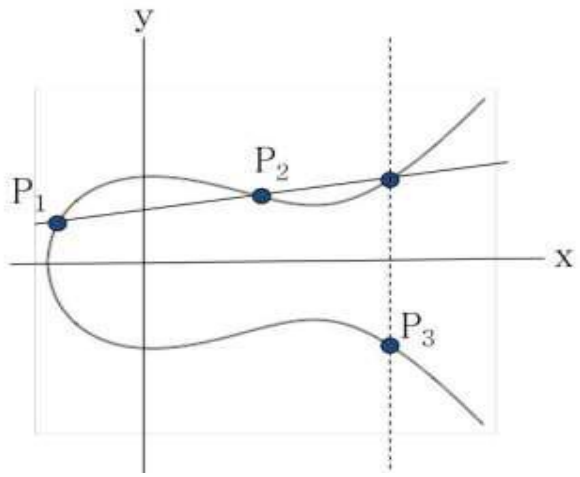

Fig 4: Elliptical Curve

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

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

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

VI. CONCLUSION AND FUTURE WORK

Elliptic Curve Cryptography provides better security and more efficient performance than the first generation public key cryptography techniques like RSA which is now in use. Although ECC’s security has not been completely evaluated, it is expected to come into universal use in different fields in the future. After comparing the RSA and ECC ciphers, the ECC has manifest to complex much less overheads compared to RSA. The ECC has many advantages due to its ability to provide the same level of security using less key size .The future of ECC looks brighter than other algorithms as today’s applications (smart cards, pagers, and cell phone etc.)not afford the overheads introduced by RSA. At least, in today’s small processing devices ECC can be applied for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to other algorithms. In future we provide different keys and security according to file.

REFERENCES

[1] Deyan Chen Hong Zhao, Data Security and Privacy Protection Issues in Cloud Computing, Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Volume: 1) ePrint23-25 March 2012the IEEE website. [Online]. Available: http://www.ieee.org/

[2] Ramgovind, S. Eloff, M.M. ; Smith, E, The management of security in Cloud computing, Information Security for South Africa (ISSA), 2010, ePrint 2-4Aug. 2010The IEEE website. [Online]. Available: http://www.ieee.org/

[3] Parsi Kalpana , Sudha Singaraju, Data Security in Cloud Computing using RSA Algorithm, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

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

[5]. Prof Swarnalata Bollavarapu, Bharat Gupta, Data Security in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering , **Volume 4, Issue 3, March 2014 ISSN: 2277 128X**, Research Paper Available online at: http://www.ijarcsse.com.

[6] Dhaval Patel, M.B.Chaudhari, Data Security In Cloud Computing Using Digital Signature,International Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014, ISSN (Online): 2347 – 4718.

[7] N. Koblitz, elliptic curve cryptosystem, mathematics of Computation, Volume 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 e-ISSN: 2231-0347 Print-ISSN: 2231-2013.

[9] Ms. Priyanka Sharda, Providing data security in cloud computing using elliptical curve cryptography, International Journal on Recent and innovation trends in computing and communication, vol.3 issue 2, 2015.

[10]. Elliptical curve cryptography, https://en.wikipedia.org/wiki/ Elliptic _curve_cryptography.

DOI 10.17148/IJARCCE.2016.5327