ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SURVEY ON CLOUD SECURITY BY DATA ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

Akanksha Tomar*, Jamvant Singh Kumare
* Research Scholar, M.Tech. (Cyber Security) Madhav Institute of Technology and Science Gwalior, M.P., India
Asst. Prof., Department of CSE&IT Madhav Institute of Technology and Science Gwalior, M.P., India

DOI: 10.5281/zenodo.225383

ABSTRACT

Cloud computing is one of the latest technology trend of the IT trade for business area. Cloud computing security converged into a demanding topic in the sector of information technology and computer science research programs. Cloud Computing is a conceptual service based technology which is used by many companies widely these days. Elliptical Curve Cryptography based algorithm provides a highly secure communication, data integrity and authentication, along with the non-repudiation communication and data confidentiality. Elliptical Curve Cryptography is known as a public key encryption technique based on the 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 techniques, Decryption, Elliptical Curve Cryptography, Digital Signature.

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.

Application
Infrastructure
Storage

A. Cryptography/ Encryption

Cryptography/ Encryption 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 to cipher 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 major problems associated with the cloud computing safety are: confidentiality, integrity and availability; shown in figure.

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.

CLOUD DATA SECURITY BY ENCRYPTION/ CRYPTOGRAPHY

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. According to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem and asymmetric cryptosystem. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), 3DES, RC5, RC6, Blowfish, Two-Fish and AES (Advanced Encryption Standard. For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret. The representatives of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptography).

RELATED WORKS

The evaluation of various symmetric key encryption algorithms, asymmetric key encryption algorithms and Digital Signature algorithms are studied based on previous researches and different resources. The symmetric encryption algorithms studied are AES, DES, 3-DES, IDES, RC5, and Blowfish. Their comparative study is based on some of the attributes such as key length, block size, cipher text, developed, security, cryptanalysis resistance, possible keys, possible ASCII printable character key is described with the help of table:

Table 1: Comparative Study of Various Symmetric Encryption Algorithms

Characteristics	**AES**	**Blow fish**	**RC5**	**IDES**	**3-DES**	**DES**
Key Length	128, 192 or 256	32 to 448 (default 128)	2040 (Max)	128	112, 168	56
Block Size	128, 192 or 256	64	32, 64 or 128	64	64	64
Cipher Text	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher
Developed	2000	1993	1994	1992	1998	1977
Security	Considered Secure	Considered Secure	Considered Secure	Proven Inadequate	Considered Secure	Proven Inadequate
Cryptanalysis Resistance	Very strong against differential, truncated differential, linear interpolation and square attack.	Strong against the standard differential and linear cryptanalysis.	Vulnerable against differential, truncated differential, linear interpolation and square attack.	Vulnerable to differential and linear cryptanalysis.	Strong against differential, truncated differential, linear interpolation and square attack.	Vulnerable to differential and linear cryptanalysis. Weak substitution table.
Possible Keys	2^{128}, 2^{192}, 2^{256}	2^{448}	2^{128}, 2^{192}, 2^{256}	2^{128}	2^{56} (all level)	2^{56}
Possible ASCII Printable Character Key	95^{16}, 95^{24}, 95^{32}	95^{16}	95^{16}, 95^{24}, 95^{32}	95^{16}	95^{7} (all level)	95^{7}
Speed	Very Fast	Fast	Slow	Slow	Slow	Very slow

It was concluded from the above comparative study, that AES encryption algorithm is faster, more efficient, and superior in terms of time consumption (encryption/decryption) and throughput under the scenario of data transfer. So it would be better to use AES scheme in encryption of data stored at other end and need to decrypt multiple time. The asymmetric encryption algorithms studied are RSA and Elliptic Curve Cryptography. These algorithms are compared based on main attribute key size with various features such as key generation time, signature generation time and signature verification time are calculated and described in a table as follows:

Table 2: Comparative Study of Asymmetric Encryption Algorithms

Characteristics	**Elliptical Curve Cryptography**	**RSA**
Key Size (bits)	163	1024
Key Generation Time	0.08s	0.16s

Signature Generation	0.15s	0.01s
Signature Verification	0.23s	0.01s

It was practically quite difficult to say which of the asymmetric encryption algorithm is better because RSA performs better in the manner while there is no requirement to generate RSA keys for every single use, but rather have fixed RSA keys. With RSA, signature generation and signature verification time is also much less than comparing to Elliptical Curve Cryptography. But Elliptical Curve Cryptography technique scores over RSA in the matter of key generation time because ECC takes less time to generate key comparing to the RSA. Elliptical Curve Cryptography is considered better option when lot of users connects to cloud based services with small session time like cloud based storage. That's why we prefer ECC as an asymmetric encryption algorithm for the cloud environment. To achieve authentication and non-repudiation purpose within cloud computing environment digital signature has assumed great significance. There are various digital signature algorithms which involves the generation of message digest (hash). MD5 and SHA-1 are well known digital signature generation algorithms and comparative study of these are described with the help of table mentioned below:

Table 3: Comparative Study of Digital Signature Algorithms

Characteristics	**MD5 (Message Digest 5)**	**SHA-512**
Message Digest Length	128	512
Attack (For original message from message digest)	2^{128}	2^{512}
Attack (Find two message for same message digest)	2^{64}	2^{256}
Successful Attack	Attempts reported	No such claims
Speed	Faster	Slow
Software Implementation	Very Easy	Easy

The study shows that MD5 is much faster than SHA-512 digital signature algorithm, but with respect to security concerns SHA-512 is more secure than MD5 and no claim of successful attacks with optimal time complexity on SHA512 has been done so far. The study of various cryptography (Symmetric/ Asymmetric) encryption and digital signature algorithms helps to choose the best one from each category to be used in proposed cryptographic module. The symmetric and asymmetric encryption algorithms to be used are AES and ECC respectively. The SHA-512 digital signature generation algorithm is used in combination with ECC asymmetric key encryption algorithm. These algorithms are described as follows:

AES (Advanced Encryption Standard): The basic steps in algorithm are stated as:
a) Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule.
b) Initial Round AddRoundKey - each byte of the state is combined with the roundkey using bitwise xor.
c) Rounds-

1) SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
2) ShiftRows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
3) MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4) AddRoundKey

d) Final Round (no MixColumns)-

1. SubBytes
2. ShiftRows
3. AddRoundKey

e) Key generation- This module handles key generation by the cryptographic module at client side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and stores a copy for it for decrypting purpose.

Elliptic Curve Cryptography (ECC) with SHA-512: An elliptic curve is given by an equation in the form of $y^2 = x^2+ax+b$, where $4a^3+27b^2 \neq 0$

The finite fields those are commonly used over primes (FP) and binary field (F2n). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDCP). This problem is defined as:

Given point X, Y on elliptic curve, find z such that X=zY. The following steps describe how ECC works with SHA-512.

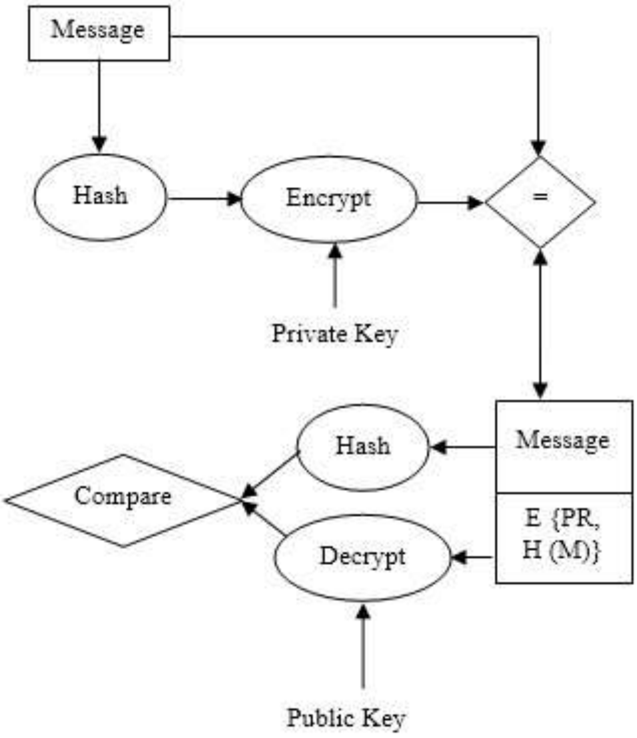
ECC key generation: To generate a public and private key pair for use in ECC communication the steps followed are:

1. Find an elliptic curve E(K), where K is a finite field such as Fp or F2n, and a find point Q on E(K). n is the order of Q.
2. Select a pseudo random number x whose value lies as $1 \leq x \leq (n - 1)$.
3. Compute point P = xQ.
4. ECC key pair is (P, x), where P is public key, and x is private key.

Signature Generation: To create a signature S for message m, using ECC key pair (P, K) over E(k), the following steps followed:

1. Generate a random number k such that
   $1 \leq k \leq (n - 1)$.
2. Compute point kQ = (x1, y1).
3. Compute r = x1 (mod n). If r = 0, go to step 1. 4. Compute k-1 (mod n).
5. Compute SHA-512(m), and convert this to an integer e.
6. Compute s = k-1(e + xr) (mod n). If s = 0, go to step 1.
7. The signature for message m is S = (r, s).

Figure 2. Basic operation of Asymmetric Key Encryption Algorithm with Digital Signature.



Signature Verification: This part verify a signature s=(r, s) for message m over a curve E(k) using the public key P performing steps:

1) Verify r and s are integers over the interval [1, n - 1].
2) Compute SHA-512(m) and convert this to an integer e.
3) Compute w = s-1(mod n).
4) Compute u1 = ew (mod n) and u2 = rw (mod n).
5) Compute X = u1Q + u2P
6) If X = 0, reject S. Otherwise, compute v = x1 (mod n).
7) Accept if and only if v = r.

CONCLUSION AND FUTURE SCOPE

Elliptical Curve Cryptography method provides the better way in cloud data security and it is more efficient in performance compare to the old generation public key cryptography techniques like RSA which are currently more deployed. Elliptical Curve Cryptography technique as a cloud data security is currently under evaluation and has not been completely evaluated yet, it is expected to come into global use featuring its presence in various fields in the nearby future. After comparing the RSA and ECC cipher texts, the ECC algorithm has manifest much less overheads compared to the RSA algorithm. The ECC has many advantages as it provides the same level of security using less key size. The future of ECC looks more future-proof in comparison to the other algorithms in current applications such as smart cards, credit/ debit cards and mobile phones overheads introduced by RSA. Now a days smaller hardware based system is a trend set and hence ECC can be applied for encryption and decryption as it requires smaller key sizes and has lesser computing complexity as compared to other algorithms. To make the ECC future-proof, different keys, key management system and security will be provided based on the need of the information characteristics.

REFERENCES

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

[2] 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.

[3] 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 ePrint 4-9, 2014.

[4] N. Koblitz, elliptic curve cryptosystem, mathematics of Computation, Volume 48-1987, PP-203-209.

[5] 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.

[6] 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.

[7] Elliptical curve cryptography https://en.Wiki pedia.org/wiki/Elliptic_Curve_Cryptography.

[8] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27,

[9] Nicholas Jansma, Brandon Arrendond, “Performance Comparison of Elliptic Curve and RSA Digital Signatures” April, 2004. [10] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, “Data Security in Cloud Computing with Elliptic Curve Cryptography” vol. 2 Issue 3, July 2012.