Cloud Security Solutions: Comparison among Various Cryptographic Algorithms

Jagriti Dhamija
Jawaharlal Nehru College of Technology, Rewa, India

Abstract-Keep Calm and Carry devices with Cloud support technology. Ask not what your cloud can do for you. Ask what you can do for your cloud. So, secure the cloud to put the data safely without any intervention by any intruder. Cloud security implementation using various cryptographic algorithms, DES, AES, RSA and ECC. This paper describes the comparison among these algorithms.

Keywords: PaaS, SaaS, LaaS, CIA, IAS, RSA, DES.

INTRODUCTION

Cloud computing is emerging as a new thing and many of the organizations are moving toward the cloud but lacking due to security reasons.

The concept of cloud computing is associated closely with Infrastructure as a Services (IaaS), Platform as a Services (PaaS), Software as a Services (SaaS) all of which means a service oriented architecture. These provides the first benefit of the cloud computing (i.e.) as there is no need to store data at end user's because it is already at some other location. So instead of buying the whole infrastructure required to run the process and save bulk of data you are just renting the assets according to your requirement. The similar idea is behind all cloud networks.

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are five types of issues raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

So, cloud security is must which will break the hindrance of the acceptance of the cloud by the organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc. are some symmetric algorithm. DES and AES are mostly used symmetric algorithms. DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange is the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. But the security algorithms which allow operations (like searching) on decrypted data are required for cloud computing, which will maintain the confidentiality of the data.

PROPOSED SYSTEM

To secure the Cloud means secure the "databases hosted by the Cloud provider". Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA). Confidentiality of data in the cloud is accomplished by encryption/ Decryption process.

Encryption/Decryption process, in modern days is considered combination of two types of algorithms. They are

(i) **Symmetric-key** algorithms cryptography such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), and Triple DES,

(ii) **Asymmetric-key** algorithms such as Rivest, Shamir, & Adleman (RSA), Elliptic Curve(EC), Diffi-Hillman(DH),

Symmetric key cryptography

Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In block cipher input is taken as a block of plaintext of fixed size depending on the type of a symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit at a time isencrypted.

1. Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit ciphertext, at the decryption site, it takes a 64-bit ciphertext and creates a 64-bit plaintext, and same 56-bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm. [1]

2. Advanced Encryption Standard (AES)

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits. AES operates on a 4×4 column-major order matrix of bytes, known as the state.

Asymmetric key cryptography

Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption.

1. RSA

RSA cryptosystem realizes the properties of the multiplicative Homomorphic encryption. Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named after its inventors. RSA uses modular exponential for encryption and decryption. RSA uses two exponents, a and b, where a is public and b is private. Let the plaintext is P and C is ciphertext, then at encryption

$C = P^a \text{mod } n$

And at decryption side $P = C^b \text{ mod } n$

n is a very large number, created during key generation process.

2. Elliptic curve cryptography (ECC)

Ecliptic curves are also used in several integer factorization algorithms that have applications in cryptography. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation,

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

along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.).This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.[2]

TABLE I. Difference between symmetric and asymmetric cryptography.

CRITERIA OF DIFFERENTI ATION	SYMMETRIC-KEY CRYPTOGRA PHY	ASYMME TRIC-KEY CRYPTOG RAPHY
Procedural	both users have the same key	Two different keys-public key and private key.
Advantages	Safer (lots of probability), and faster.	c other people read the encrypted message. No problem for distributing the key.
Dis- advantages	One-time transactions. Repeatedly change the key at both sides.	Big and slow.

COMPARISION

A common aim for cryptographic algorithms is to provide confidentiality and authentication. A cryptographic algorithm is computationally secured if it cannot be broken with standard resources. An efficient cryptosystem can produce best possible results if key size is comparable to the size of the packet to be transmitted over the network. Algorithm based on parameters like key-length, block-size, type and features. [3]

TABLE II. Comparison between symmetric and asymmetric algorithms.

Factors	**DES**	**AES**	**RSA**	**ECC**
Contributor	IBM 75	Rijman, Joan	Rivest, Shamir 78	Neal Koblitz,Victor S. Miller
Key Length	56-bits	128,192, and 256	Based on No. of bit in N=p*q	135 bits
Block Size	64-bits	128 bits	Variant	Variant
Security Rate	Not enough	Excellent	Good	Less
Execution Time	Slow	Faster	Slowest	Fastest

CONCLUSION

While cost and ease of use are two great benefits of cloud computing, there are significant security concerns that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments.

[4] To address these concerns, the cloud provider must develop sufficient controls to provide the same or a greater level of security than the organization would have if the cloud were not used. Security is a very important aspect of cloud computing. Resources can be shared but the extent of user authorization varies. Files can be uploaded in encrypted form and using the concept of keys can be downloaded.

FUTURE SCOPE

Using various algorithms as described cloud security can be ensured in a real-time environment. IT Companies can benefit a lot from cloud computing as all the data can be centralized in a protective environment.

REFERENCES

[1]. Rashmi Nigoti, ManojJhuria, Dr. Shailendra Singh, A Survey of Cryptographic Algorithms for Cloud Computing, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Madhya Pradesh,2010.

[2]. K.S. Suresh, Prof K.V. Prasad, Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Hyderabad, 10, October 2012.

[3]. Dr. L. Arockiam, S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[4]. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, Ensuring Data Storage Security in Cloud Computing.