Data Security on Cloud Computing

K.Pranathi
Assistant Professor, Department of Information Technology
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India

M.Sai Sri Lakshmi Yellari
Department of Information Technology
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India

Abstract- Generally, data can be stored in many types of storage devices like primary, secondary and tertiary. As the data is growing large and we want the data to be, portable we have moved to cloud computing because of its versatality.Cloud Computing is the use of activity of using computer Hardware and Software. It is a set of IT services that are provided to a customer over a network and third party providers provide these services who own the infrastructure. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), or software as a service (SaaS) We are very well concerned about the security in each and every aspect we work. Therefore, security algorithms very well solve the issues arise for the data to be stored (or) retrieved over a cloud. In this paper I would like to discuss about the security issues, security algorithms and the most trending algorithms implemented to resolve the related security issues.

Keywords – Cloud computing, Enhancing Data Security, Security Issues, Security Algorithms.

I. INTRODUCTION

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements [5].

The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities [5].

Coming to data storage, data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used [5]. The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.

A number of data protections and data security techniques have been proposed in the research field of cloud computing. However, data protection related techniques need to be further enhanced.

The moment we hear the word 'Data' we are concerned about the issues raised with it. The issues could be like Data Confidentiality, Data Integrity, Data Availability, Data location, Data relocation, Data privacy etc. Often these concerns are termed as "Data Security Issues in Cloud".

Data Confidentiality: The cloud seeker should be assured that data hosted on the cloud will be confidential [5].

Data Integrity: The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

Data Availability: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

Data Location: Cloud Computing offers a high degree of data mobility. This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information [1].
Data Relocation: Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources.
Data Privacy: Privacy is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively.

The security issues raised can be resolved using various algorithms. Based on the level of security the user wish to provide or the technique he would like to implement for his data over a cloud varies, involving implementation of different algorithms.

The algorithms were categorized into two different types:

- ➢ Symmetric
- ➢ Asymmetric

SYMMETRIC ALGORITHMS: Symmetric algorithms are those which make use of only a single key for encryption and decryption purpose.
There are many algorithms which come under the category of Symmetric.
DES: Data Encryption Standard is one of the most widely accepted, publicly available cryptographic systems. It was developed by IBM in the 1970s but was later adopted by the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46).
Advantages: The Avalanche Effect is the major advantage which states that "A slight in a char or bit change in the plaintext will drastically change the cipher text" [3].
Disadvantages: Memory Requirement and Simulation Time is more in case of DES.

AES: Advanced Encryption Standard, is the new encryption standard recommended by NIST to replace DES in 2001 [3]. AES is one the most efficient symmetric algorithm.
Advantages:

- It provides strong security from the attackers.
- But as the years passed by it was prone to a few attacks which were lesser when compared to DES, till date the only attack on it was Brute Force attack.

Disadvantages:

- The major drawback is that it could not withstand with the attacks like Brute Force, Linear crypt Analysis, because during its design this attack wasn't invented.

ASYMMETRIC ALGORITHMS: Asymmetric algorithms are those which make use of two or more keys (i.e.) Public and Private Keys for the purpose of encryption and decryption.
DIFFIE-HELLMAN: It is one of the most popular Asymmetric algorithms before RSA which is named after the Whitfield Diffie and Martin Hellman. It makes use of two keys namely: Private and Public. This uses a shared secret key for data transmission.
Advantages:

- The CIA rule (Confidentiality, Integrity and Authentication) makes the biggest advantage for opting this algorithm in security systems [2].

Disadvantages:

- The Time consuming nature and its Weak Key.

ELGAMAL ALGORITHM:
ElGamal technique is used for both:

- o Digital Signature
- o Encryption [4].

Advantages:

- El-Gamal has Homomorphic property that makes it useful in application like e-voting

Disadvantages:

- Need for randomness
- Slow speed, especially for signing.
- Message expansion by the factor of two takes place during encryption [4].

II. Proposed Algorithm

RSA ALGORITHM:

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977 [1]. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it.

RSA ON CLOUD:

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. Encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

KEY GENERATION:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user [1].

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø (n) and greatest common divisor of e, Ø (n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: d = e-1(mod Ø (n)) i.e., d is multiplicative inverse of e mod Ø(n).
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e., (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e., (d, n).

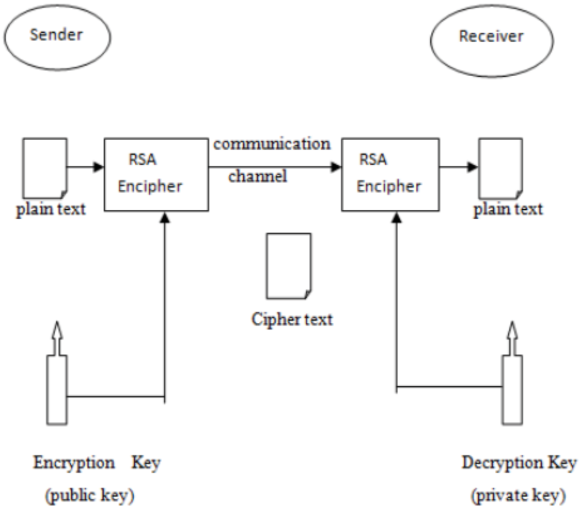

Figure 1. Overview of RSA Algorithm

ENCRYPTION:

Encryption is the process of converting original plain text (data) into cipher text (data) [1].

Steps:

1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is C = me (mod n).
4. This cipher text or encrypted data is now stored with the Cloud service provider.

DECRYPTION:
Decryption is the process of converting the cipher text (data) to the original plain text (data).
Steps:
1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e.,
3. The Cloud user then decrypts the data by computing, m = Cd (mod n).
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

Merits of RSA on Cloud:
➢ The biggest advantage of using RSA on Cloud for Data Security is its Public Key Encryption.
➢ It provides increased Security and Convenience for the user for storing and retrieving data.
➢ It is a fast encryption algorithm.
➢ Provides digital signatures that cannot be repudiated [4].

Demerits of RSA on Cloud:
➢ The data can be vulnerable to impersonation if hacked.
➢ Slower than secret key method, but can be used in conjunction with the secret key to make it more efficient [4].

III. EXPERIMENT AND RESULT

This paper has made detailed study about the types of algorithms. The type of encryptions, decryptions they followed and the extent to which they can provide security for the data resisting against the maximum number of attacks occur on them. As DES algorithm has prone to numerous attacks being the popular algorithm for encryption is ruled out besides having AES algorithm which has been the most efficient algorithm although with more number of rounds it has to undergo, also Diffie-Hellman and ElGamal algorithms for their weak keys have been ruled out. Opting RSA algorithm for providing Data Security on Cloud for better user access and the Confidentiality, Integrity and Authentication it provides, made it a better option so far for its implementation on Cloud for Data Security.

IV.CONCLUSION

Cloud Computing is the latest buzz word in the world of IT. Security is a major requirement in cloud computing while we talk about data storage. Security algorithms mentioned for advanced encryption and decryption can be implemented in future to enhance security over the network. Cloud Computing is the phenomenon of separating applications from hardware and providing an easy way to deploy on demanded server. The functioning of Cloud Computing is greatly affected by issues such as that of data security, integrity, theft, loss and presence of infected applications. To solve these issues various algorithms such as DES, AES, RSA, Diffie-Hellman and many more algorithms are there so that any unauthorized user trying to access the confidential data will not be allowed to access the cloud.

REFERENCES

[1] Parsi Kalpana, et al, “Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN: 2278-5841, Vol 01, Issue 4, September 2012.

[2] Punnam .V. Maitri, Aruna Varma, “Enhancing File Security using Cryptography Algorithms in Cloud Computing: A Survey”, International Journal of Innovative Research in Computer and Communication Engineering, IJIRCE, ISSN: 2320-9798, Vol 3, Issue 10, October 2015.

[3] Gurpreet Singh, Supriya,” A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security “, International Journal of Computer Applications, IJCA, ISSN: 0975-8887, Vol 67, No.19, April 2013.

[4] Prof Swarnalata Bollavarapu, Bharat Gupta,” Data Security in Cloud Computing “, International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSSE, ISSN: 2277 128X, Volume 4, Issue 3, March 2014.

[5] Yunchuan Sun, Junsheng Zhang,Yongping Xiong, and Guangyu Zhu,” Review Article on Data Security and Privacy in Cloud Computing”, International Journal of Distributed Sensor Networks, IJDSN, ISSN: 190903, Volume 2014 (2014), 9 pages, July 2014.