International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 3
ISSN: 2454-4248
373 – 375

A Review of Various Security Techniques in Cloud computing

Kulwinder Kaur
Research Scholar
Punjabi University
Patiala, India
kulwinderdhillon286@gmail.com

***Abstract*—**Cloud computing is the major area of research. In this paper our aim is to study the existing literature of various security algorithms in cloud computing. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the third party so authentication of client becomes a mandatory task. In this paper, we discuss a number of existing techniques used to provide security in the field of cloud computing on the basis of different parameters.

Keywords*—Cloud, Make span, Computing, Energy, Security*

*****

I. INTRODUCTION

Cloud computing is growing fast with time. Cloud computing illustrate Information Technology as a fundamentally diverse operating model that takes advantage of the maturity of web applications and networks and the rising interoperability of computing systems to provide IT services. Data security is becoming a fundamental obstruction in cloud computing. There are some kind of solution that are provide some security with model, some technology. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Security is the major issue in the adoption of cloud computing. Many cryptographic algorithms are available to solve data security issue in cloud. Algorithms hide data from unauthorized users. Encryption Algorithms have vital role in the data security of cloud computing. Examples of algorithms are AES, DES, RSA, Homomorphic, etc. Two operations performed by these algorithms are encryption and decryption. Encryption is the process of converting data into scrambled form and Decryption is the process of converting data from scrambled form to human readable form. Symmetric algorithms use one key for encryption and decryption while Asymmetric algorithms use two keys for encryption and organizations can easily deliver any new application/product at the release time itself.

A. Cryptography

It is a science used to secure sensitive data. Confidentiality is the fundamental security serviceprovided by cryptography, keeping data invisible to unauthorized users. Components of cryptosystem are follows:

1. **Plaintext:** Original form of data, data to be protected during transmission and storage. Cipher text: It is the unreadable form of the plaintext after encryption operation. Encryption Algorithm: Used to convert plaintext to cipher text, it is a mathematical process.
2. **Decryption Algorithm:** It performs reverse operation of encryption algorithm, convert cipher text to plaintext.
3. **Encryption Key:** It is a value used by sender with algorithm to convert plaintext to cipher text. Decryption Key: It is a value used by receiver with algorithm to convert cipher text to plaintext.

B. Encryption Algorithms for Cloud Security

Encryption algorithms have vital role in the field of cloud security. Many algorithms are available for cloud security. Most useful algorithms for cloud security are discussed below.

1.Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for

 ISSN: 2454-4248
373 – 375

both encryptionand decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits.Entire plaintext is divided into blocks of 64bit size; last block is padded if necessary. Multiplepermutations and substitutions are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES algorithm consists of two permutations (P-boxes) and sixteen Feistel rounds. Entire operation can divided into three phase. First phase is Initial permutation and last phase is the final permutations.

i Initial permutation rearranges the bits of 64-bit plaintext. It is not using any keys, working in a predefined form.

ii There are 16 fiestel rounds in second phase. Each round uses a different 48-bit round keyapplies to the plaintext bits to produce a 64-bit output, generated according to a predefined algorithm. The round-key generator generates sixteen 48-bit keys out of a 56-bit cipher key.

iii Finally last phase perform Final permutation, reverse operation of initial permutation and the output is 64-bit cipher text.

2. Advanced Encryption Standard (AES)

AES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). Most adopted symmetric encryption is AES. It operates computation on bytes rather than bits, treats 128 bits of plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. It operates on entire data block by using substitutions and permutations. The key size used for an AES cipher specifies the number of transformation rounds used in the encryption process [8][9].Possible keys and number of rounds are as following:

- 10 rounds for 128-bit keys.
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Major advantages of AES over DES are:

1. Data block size is 128 bits.
2. Key size 128/192/256 bits depending on version.
3. Most CPUs now include hardware AES support making it very fast.
4. It uses substitution and permutations.
5. Possible keys are 2128 , 2192 and 2256 [10]
6. More secure than DES.
7. Most adopted symmetric encryption algorithm.

3. Rivest-Shamir-Adleman (RSA)

RSA is a public key cipher developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977. It ismost popular asymmetric key cryptographic algorithm. This algorithm uses various data block size and various size keys. It has asymmetric keys for both encryption and decryption. It uses two prime numbers to generate the public and private keys. These two different keys are used for encryption and decryption purpose [11]. This algorithm can be broadly classified in to three stages; key generation by using two prime numbers, encryption and decryption.

RSA today is used in hundreds of software products and can be used for key exchange, digital signatures, or encryption of small blocks of data [12]. This algorithm is mainly used for secure communication and authentication upon an open communication channel.

While comparing the performance of RSA algorithm with DES and DES, when we use small values of p &q (prime numbers) are selected for the designing of key, then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES[12]. Operation speed of RSA Encryption algorithms is slow compare to symmetric algorithms; moreover it is not secure than DES.

4. Homomorphic Algorithm

It is an encryption algorithm that provides remarkable computation facility over encrypted data (cipher text) and return encrypted result. This algorithm can solve many issues related to security and confidentiality issues. In this algorithm encryption and decryption taking place in client site and provider site operates upon encrypted data. This can solve threat while transferring data between client and service provider, it hide plaintext from service provider, provider operates upon ciphertext only.

Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without using the original data. For plaintexts X1 and X2 and corresponding ciphertext Y1 and Y2, a Homomorphic encryption scheme permits the computation of X1 Θ X2 from Y1 and Y2 without using P1 Θ P2.The cryptosystem is multiplicative or additive Homomorphic depending upon the operation Θ which can be multiplication or addition[13].

II. LITERATURE SURVEY

It was mentioned in [10] that AES is faster and more efficient symmetric algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. This provides high security over open network but key transfer is the major issue in symmetric algorithms.

Based on the text files used and the experimental result it was concluded [11] that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm, but RSA Encryption algorithms

 ISSN: 2454-4248
373 – 375

consume a significant amount of computing resources such as CPU time, memory, and battery power.

Comparison of secret key and public key based DES and RSA algorithms [12], it clears that RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography. But it does not solve all the security infrastructure .So DES is used. RSA and DES differ from each other in certain features.

Paper [13] specifies that RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES.

According to research done [13] and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data.

Based on the text files used [14] and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. We also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

III. CONCLUSION

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges still exist in this technology. Security is the most challenging issue in this technology. In this paper we have discussed various encryption algorithms to overcome this security issue, deals with advantages and disadvantages of these algorithms. Here we conclude that homomorphic algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. The ability of homomorphic algorithm to perform operations on encrypted data enables high security than other algorithms such as RSA, DES, AES. Future work is to implement hardware or software technique with homomorphic algorithm to provide protection on cloud from any type of security attack.

REFERENCES

[1] Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360-Degree Compared CoRR. abs/0901.0131.

[2] Satyakam Rahul, Sharda, “Cloud Computing: Advantages and Security Challenges” International Journal of Information and Computation Technology, vol. 03, 2013

[3] Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud- computing-security-risks-853.

[4] Anca apostu, Florina puican, Geanina ularu, George suciu, Gyorgy todoran, “Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud”, Recent Advances in Applied Computer Science and Digital Services

[5] Srinivasa rao v, Nageswara rao n k, E Kusuma kumari, “Cloud Computing: An Overview”, Journal of Theoretical and Applied Information Technology.

[6] Data Remanence, https://en.wikipedia.org/wiki/Data_remanence.

[7] Vijay Kumar, “Brief Review on Cloud Computing”, International Journal of Computer Science and Mobile Computing, vol. 5, September 2016,

[8] Rijndael.Advanced Encryption Standard (AES). FIPS. November 23, 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf

[9] Hesham Darwish, “ Avanced algorithm design and analysis”. IJCSMC-2017, volume 5, Issue-4.

[10] Shraddha Soni, Himani Agrawal , Dr. (Mrs.) Monisha Sharma, “Analysis and Comparison between AES and DES Cryptographic Algorithm”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

[11] Shashi Mehrotra Seth, Rajan Mishra, “Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, June 2011

[12] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, “Comparative Analysis between DES and RSA Algorithm’s”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

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

[14] Dr. Prerna Mahajan & Abhishek Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security”,Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[15] Liam Morris, “Analysis of Partially and Fully Homomorphic Encryption”,ochester Institute of Technology, Rochester, New York

[16] Iram Ahmad, Archana Khandekar, “Homomorphic Encryption Method Applied to Cloud Computing”, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530