ISSN:0975-9646

Scrutiny of Different Encryption Algorithms in Cloud Computing

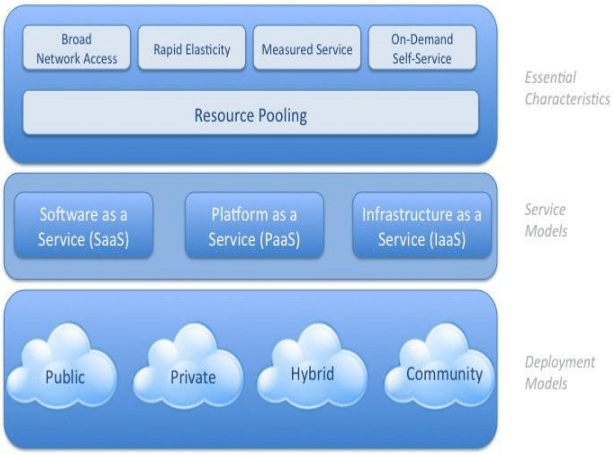
Shakeel Juman T.P,
Assistant Professor in Computer Science and Application, CCSIT

Abstract: Cloud computing is now a fast and evolving technology; it is the technology for the coming generation. This technology has completely transformed the face of traditional computing technologies. It offers a lot of utilities to the IT field, though it has to face many challenges to attain its maturity level. This paper deals with the various benefits and major security challenges of cloud computing, it also highlights many cryptographic encryption algorithms as the major solution for security challenges. Moreover this paper compares the efficiency of each algorithm in cloud computing.

INTRODUCTION

Cloud computing is the essential part in the emerging technology. It is the fastest growing technology, it performs great services over the internet. There are three types of services in cloud computing which are used for deployment of the application on the cloud. It can offer many facilities to the business such as resources, infrastructure, platform etc by spending money on demand basis over network with the functionality of increase or decrease the requirements. This technology can always meet any IT requirements. It can offer most of the hardware and software facilities and requirements for the companies for storing, creating, managing and running consumer applications on cloud in lease or rent basis, it provides resources as a service to multiple consumers by virtualization. This technology helps many IT organizations to begin business without huge economical capital, slowly move to leading organization in the industry. It can offer facilities irrespective of the size of establishments or organizations. These offers gave new face to the computing technology. According to NIST, Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Various cloud service providers and Big players are Amazon, Google, IBM, Microsoft, and Salesforce.com, are different cloud service establishments who provide their cloud infrastructure for services.

As mentioned above, they offer many services than traditional IT models but from the consumer perspective, Cloud computing security concerns continue to be a major barrier to adopting this technology [2]. Consumers are not ready to put their valuable data in cloud; they feel more their infrastructure more secure than the cloud infrastructure. Preserving data in an open network will create suspicion in the minds of the consumers on the secrecy, availability, misuse of information of their valuable data. Most of the consumers are unaware about the security measures, operations in cloud etc. According to a survey carried out by Gartner [3], more than 70% of Chief Technical Officers believed that the primary reason for not using cloud computing services is that of the data security and privacy concerns.



Security is the major issue in the adoption of cloud computing. Many cryptographic algorithms are available to provide data security in cloud. Algorithms conceal data from unauthorized users. Encryption Algorithms have great 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 separate keys for encryption and decryption.

Benefits of Cloud computing

Numerous benefits are offered by cloud computing. Major benefits are explained below.

1. **Low Cost:** Cloud computing provides facility to start an IT company with less effort and initial cost. Cloud computing services are shared by multiple consumers in the world. It reduces the cost of service due to large number of consumers. It charges amount depending upon the usage of infrastructure, platform and other services. This helps consumers to reduce the cost by specifying the exact requirements. Companies can easily increase or decrease their demand for services according to the performance of their company in market.
2. **Scalability and Flexibility:**
   Cloud computing can help companies to start with a small set up and develop to a large condition fairly

rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands. Moreover, cloud computing is efficient to meet any peak time requirement by setting up with high capacity servers, storages etc. This facility helps consumers to meet any type of requirement irrespective of the size of project.

3. **Backup and Recovery:**
   Since all the data is stored in the cloud, backing it up and restoring the same is comparatively much easier than storing the same on a physical device [4]. Also it has many techniques to recover it from any type of disaster; most efficient and new techniques are being adopted by most cloud service providers to meet any type of disaster or data loss. Cloud Providers can get any type of technical and other support faster than any individually set up organizations irrespective of their geographical limitations.
4. **Broad network Access:**
   loud services are delivered through open network (Internet), it can be easily accessible at any time anywhere in the world. These facilities can be accessed by various devices such as mobile phones, laptops, PDAs etc with different platforms. Consumers can access their files and other applications on their finger tips at anytime from anywhere by using their mobiles. This has increased the rate of adopting cloud computing technology immensely.
5. **Multi sharing:**
   Cloud Computing provides services by sharing of architecture and other applications over Internet for single and multiple users by using virtualization and multi-tenancy. With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure [5].
6. **Collaboration:**
   Major projects or applications are delivered by the effort of multiple group of people working together. Cloud computing presents a convenient and easy way to work group of people together on a common project or applications in an effective manner.
7. **Deliver New Services:**
   Cloud services are provided by multi-national companies like Amazon, Google, IBM, Microsoft, Salesforce.com, etc. These organizations can easily deliver any new application/product at the release time itself.

Challenges of Cloud Computing

Cloud computing provides many aforesaid benefits, still cloud computing has many challenges. While changing from traditional computing to cloud computing, companies must be aware about both the benefits and challenges of cloud computing. While observing these challenges, security of data is the most tedious work in cloud computing. According to a survey carried out by Gartner [3], more than 70% of Chief Technical Officers believed that the primary reason for not using cloud computing services is that of the data security and privacy concerns. Convincing the organizations especially small ones about security concern is a tedious work; they are not ready to throw away their infrastructure and move immediately to cloud. Most of the organizations are closely watching this issue and are not ready to change to cloud space, this is the main reason in the lack of maturity level of cloud computing. Some of the security challenges are discussed below.

1. Privacy of data:

Privacy of data is the key security concern for cloud computing. Most of the organizations feel more comfort while putting valuable data in their site than cloud space. Consumers do not have any idea about the location of data, transfer of date, operations on cloud, etc. Most of the organizations are unaware of security mechanism implemented by service providers. Many consumers arise questions like :

1. Which are the organizations sharing services.
2. How creation and back-up of files take place.
3. What happens to the deleted files?
4. Which type of consumers can access data?
5. Questions regarding the Location of data.
6. Etc.

2. Confidentiality of data:

Confidentiality is related to data privacy; it ensures that the data is visible only to the authorized users. It is very difficult as the virtualization and multi tenancy properties that multiple consumers who share the hardware and the software simultaneously in a distributed network. Confidentiality is the responsibility of the service provider. The common solution to the confidentiality is encryption. A lot of symmetric and asymmetric algorithms are available for data confidentiality, even though the encryption and the decryption are the solution to the confidentiality, many questions arise related to this.

1. Where the encryption and decryption take place (client side or cloud side).
2. How one can search the data in an encrypted form.
3. What are the threats while the transfer of data from client to cloud?
4. Is there any miss use of data by service provider?
5. Is there any miss use of key by service provider?
6. Etc.

3. Data Remanenece:

Data should be deleted from cloud after the life-cycle, or the memory should be reformatted or recycled. The reformation of storage media does not remove the previously written data from the media, but it can be accessed or recovered from the media later. No clear standard is available for the recycle of the storage media. This remaining data makes difficult the vacation of hardware resources from the cloud. Most consumers don’t know the allotted resources and storage space. Due to this issue consumers are locked in one service provider.

Various techniques have been developed to counter data Remanenece. These techniques are classified as cleaning, purging/sanitizing, or destruction. Specific methods include overwriting, degaussing, encryption, and media destruction [6].

4. Data integrity:

Preservation of information from loss or modification by unauthorized users is referred as data integrity. Multiple organizations are sharing the application or platform by multi-tenancy, consumers working on same work may share data and it may be modified by any other unauthorized user sharing the application or platform in the cloud, this causes the integrity failure. As data is the base for providing cloud computing services, data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task [7].

5. Transmission of data:

Most of the time the data is being transferred between consumer and cloud. Initially data is sent from the client site to cloud, data is returned from cloud to client after queries during the operation. Encryption is used to provide protection while the transmission of data. Most of the time data is transferred without encryption as a lot of time is required for encryption and decryption for each operation upon data. During transfer an attacker can trace the communication, interrupt the data transfer and miss use the data, etc. Homomorphic algorithm allows to process data in an encrypted form, even though there is a chance of data transfer interruption, change the data transfer and other issues.

6. Malicious Insiders:

Malicious insiders are the authorized employees, these users are appointed for managing and maintaining cloud by cloud service provider. These users sometimes steal or corrupt the sensitive data of organizations in the cloud and convey this sensitive information to other organizations sharing the same cloud. These malicious insiders may get payment for this malicious work. Sometimes the service provider will not able to take any action against these employees.

Cryptography

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

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.

Decryption Algorithm: It performs reverse operation of encryption algorithm, convert cipher text to plaintext.

Encryption Key: It is a value used by the sender with algorithm to convert plain text to cipher text.

Decryption Key: It is a value used by receiver with algorithm to convert cipher text to plaintext.

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 both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits.

The entire plaintext is divided into blocks of 64 bit size; last block is padded if necessary. Multiple 6 permutations 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 be divided into three phases. The First phase is initial permutation and the last phase is the final permutations.

1. Initial permutation rearranges the bits of 64-bit plaintext. It is not using any keys, working in a predefined form.
2. There are 16 fiestel rounds in second phase. Each round uses a different 48-bit round key applies 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.
3. Finally last phase performs 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 makes 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 is most 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 into 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 are slow compared to symmetric algorithms, moreover they are not securer than DES.

4. Homomorphic Algorithm

It is an encryption algorithm that offers remarkable computation facility over encrypted data (cipher text) and return encrypted result. This algorithm can solve many issues related to security and confidentiality. In this algorithm encryption and decryption that take place in client site and provider site operate upon encrypted data. This can solve threat while transferring data between client and service provider, it hides plaintext from service provider, provider operates upon cipher text 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 cipher text 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 the multiplication or addition[13].

Literature Survey

It is mentioned in [10] that AES is quicker and more efficient symmetric algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. This offers high security over open network, but key transfer is the major issue in symmetric algorithms 67 based on the text files used and the experimental result. It is 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 consume a remarkable amount of computing resources such as CPU time, memory, and battery power. Comparison of secret key and public key based on 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 and therefore is 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 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, through put and avalanche effect. The Security provided by these algorithms can be extended 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. It was concluded [15] that Homomorphic cryptosystems allow for the same level of privacy as any other cryptosystem, while also allowing for operations to be performed on the data without the need to see the actual data. Complete privacy between client and server would not be possible without any decreased functionality. Such systems could be applied to nearly anything that requires computation, such as voting, banking, cloud computing, and many others. It is concluded [16] that Homomorphic encryption is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. Security of cloud computing based on fully Homomorphic encryption is a new concept of security which enables to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data.

CONCLUSION

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges are still existing 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). *C*loud 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]. Ancaapostu, Florina puican, Geaninaularu, George suciu, Gyorgytodoran, “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]. Srinivasarao v, Nageswararao n k, E Kusumakumari, “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]. HeshamDarwish, “ Avanced algorithm design and analysis”. NasarulIslam.K.V*et al*, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017, pg. 90-97

[10]. Shraddha Soni, HimaniAgrawal , 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. SudeshJakhar, 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, ArchanaKhandekar, “Homomorphic Encryption Method Applied to Cloud Computing”, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530

[17]. Sumitra, “Comparative Analysis of AES and DES security Algorithms”, InternationalJournal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, ISSN 2250-3153