© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

# A Review on Security Algorithms in Cloud Computing

**Archana M[1], Dr.Mallikarjuna Shastry[2]**

[1]Research Scholar, School of Computing and Information Technology REVA University, Bangalore, Karnataka, India

[2]Professor, School of Computing and Information Technology REVA University, Bangalore, Karnataka, India

## ABSTRACT

At present, cloud computing is the fastest growing technology in today's world. Cloud computing is a model that provides the services based on as-needed and when-needed basis. Cloud computing provides online information storage, infrastructure and application. Many organizations shift towards cloud computing due to its benefits of less hardware maintenance and reduced expenditure start-up cost and at the same time, cloud computing offers many hazards. Network and Internet applications are growing very fast, since the need to secure these applications are very fast. For this purpose cryptography algorithms (symmetric & Asymmetric) are proposed. The use of relevant algorithm deals with the level of data safety in cloud because data security in cloud computing is a serious issue as the data centers are located worldwide. Authentication is the most essential procedure to ensure the cloud data in a secured manner. However, strong user authentication is the main requirement for cloud computing that reduces the unauthorized user access of data on cloud. Data security is a more important issue of cloud computing. Thus, the need to ensure the safety of information. Here in this survey paper, I have presented encryption based security algorithms for cloud computing.

**Keywords:** Cloud Computing, Security Issues, Symmetric and Asymmetric algorithms

## I. INTRODUCTION

The term cloud refers to the web or internet. Cloud computing is a metaphor for transferring the information services from the internet. With the help of web-based tools and applications, information is transmitted to the internet [1]. Cloud computing is a compilation of existing approaches and technologies, Prepacked among a brand infrastructure paradigm that provides improved measurability, elasticity, business process, quicker startup time, reduced management prices and just-in-time accessibility of resources. Resources include database, software, service and server and so on [2].

In cloud computing, cloud actors play a major role. Cloud actors are referred as cloud agents. Two cloud actors are used. They are cloud provider and cloud consumer. A cloud provider is an organization responsible for providing cloud services to cloud consumers based on service level agreement (SLA). Cloud provider is also referred as data owner. Examples of cloud providers are Google, Amazon Web Service, IBM, Microsoft, eBay, Salesforce.com and so on. Cloud provider offers the owned IT resources to the cloud consumers for lease. Cloud consumer is an organization that uses IT resources based on the contract with a cloud provider. Cloud consumer is also referred as a client.

## II. CHARACTERISTICS OF CLOUD COMPUTING

The important features of cloud computing involves:

A. On-demand self service Cloud computing provides the resources to the end users in a simple and flexible way. Initially, users use the limited resources and based on the need, users utilize more resources. Based on the resources used, users need to pay money. This on-demand self service is also called as a utility service.[3]

B. A broad network access The ability of the cloud users to use the cloud services that can be widely available. This characteristic is referred as ubiquitous access. Ubiquitous access requires a support for the particular devices, interfaces, protocols and technologies. To enable this access, cloud services should satisfy the needs of the cloud users.[3]

C. Rapid elasticity Ability of cloud computing that can be transparently extend the IT resources based on the request that has been given by cloud consumers or cloud providers. Wide range of scalability is achieved by the cloud providers with the vast range of IT resources. [3]

D. Resource pooling Cloud provider stores the IT resources in the cloud. Based on the needs of the end users, resources can be dynamically assigned and reassigned. Multiple cloud consumers can use a large amount of IT resources that has been stored by the cloud provider. Multi-tenancy achieves resource pooling.[3]

E. Measured service The cloud platform maintains the use of IT resources that has been used by cloud consumers. This feature is closely related to the on-demand service characteristic. According to the resources used by the cloud consumers, cloud providers charge the cloud consumers. [3]

## III. SERVICE MODELS OF CLOUD COMPUTING

Infrastructure as a Service: IaaS provide on-demand provisioning of infrastructural resources and does not manage or control the infrastructure and only manage and control the storage, application and selected network components. The cloud owner who offers IaaS is called an IaaS provider. Examples: Amazon EC2 .

Platform as a Service: PaaS providing software development frameworks and platform layer resources including operating system support. In PaaS user controls their application and does not manage servers and storage. Examples: Google App Engine,Microsoft Windows Azure etc.

Software as a Service: SaaS providing on demand applications all over the Internet. In SaaS user does not control or manage the servers, storage, network and application. Examples: Rack space etc.

## IV. CLOUD SECURITY AND ITS ISSUES

The main objective of cloud computing is data sharing. Since all users can share the data that have been stored in the cloud at that time there is a possibility of breaching information. In order to prevent the information leakage, cloud security is used. Cloud security is an approach of protecting the data in the cloud computing environment.

Security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud. Cloud Computing infrastructure uses new technologies and services, most of which haven‛t been fully evaluated with respect to the security. Cloud Computing has several major issues and concerns, such as data security, trust, expectations, regulations, and performances issues. One issue with cloud computing is that the management of the data which might not be fully trustworthy; the risk of malicious insiders in the cloud and the failure of cloud services have received a strong attention by companies.

Security Issues In cloud computing,

1. Privacy and Confidentiality
2. Data Integrity
3. Data Availability

security must happen on two levels [4][5]. The one is on provider level and another is on customer level.

Security on provider level Provider need to check that the server is secured from the external threats [5]. A cloud is good if there is a security offered by the provider to the customers.

Security on user level User needs to check that the data received by the provider are without any loss [5].

## V. SECURITY ALGORITHMS IN CLOUD COMPUTING

To provide data security in cloud computing there are all the more existing methods. Which utilizes encryption and decoding strategies for well-being and security with client information on the cloud? Here we are utilizing symmetric and asymmetric encryption algorithms[26]. The symmetric encryption method is having only one key that is used to encrypt and decrypt the data. Another method is asymmetric encryption that is having two key one is private key and another one public key. Private Key is used for decryption and public key is used for encryption. [6]. The classification is shown in figure 1.

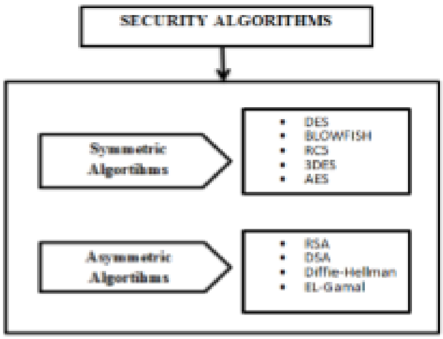


**Figure 1.** Security Algorithms

### 4.1 Symmetric Technique

### 4.1.1 DES

DES stands for Data Encryption Standard established in 1977. It applies a 56-bit key to each 64bit block of data. It was the first encryption standard to be approved by NIST. This Method can run in number of modes and requires 16 rounds or controls, even though this is designed with "strong" encryption. We have used DES algorithm with destruction-editing approach for providing data security with integrity [7]. Each round in the deals with uses a separate 48-bit round key which is produced from the consistent cipher key according to the DES techniques [8].The Data Encryption Standard (DES) is a formerly transcendent symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of present day cryptographic systems.DES is the block cipher an algorithm that takes a fixed length string of plaintext bits and changes into a series of muddled operations into another ciphertext series of bits with the same length. On account of DES, for the most part, the block size is 64 bits. DES additionally utilizes a key to altering the change, so that decryption must be performed by the individuals who know the specific key used to encrypt. At the present DES issued to be unconfident for multiple applications, and therefore it has been replaced by the Advanced Encryption Standard (AES) [9].

### 4.1.2 BLOWFISH

It is symmetric encryption algorithm. It have 64 bit block cipher developed by Bruce Schneider; enhanced for 32-bit mainframes with huge data stores, it is greatly faster than DES on a Power PC-class machine. Key lengths can differ from 32 to 448 bits in range. Also it‘s have 16 rounds. Blowfish, accessible easily and developed as an alternate for DES or IDEA which is in use in a large number of production [10].

### 4.1.3 RC5

It is symmetric encryption algorithm that deals with 128 bit block cipher based upon, and a development done, RC5. Also its have 12 rounds. The utilization of RC5 algorithm for encryption, cloud computing can be connected to the data transmission security. Transmission of data will be encrypted; regardless of the fact that the data is stolen, there is no relating key that can't be restored [11].

### 4.1.4 3DES

In Triple DES (3DES) Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher encryption is discussed with the development of the Data Encryption Standard (DES) cipher techniques. TDES uses a block size of 64 bits and operate 48 processing round corresponding to DES. In 3DES three times iteration is produced to improve the encryption and security level [10]. It makes three encryption and decryption permits done the block using DES 56 bit keys [10].

#### 4.1.5 AES

Advanced Encryption Standard (AES) uses a symmetric key encryption design known as called Rijnadael, a block cipher proposed by Belgian cryptographers Joan Daemen and Vincent Rijmen [10]. The key size can have variable lengths such as 128,192 or 256 bits. The default key size is 256 bits. AES encryption standards are very fast, it is flexible and effective than DES. It has had total 14 rounds contingent on the key sizes which are used in [6]. It is one of the very regularly used and is available for utilizing the data secure purposes; the algorithm depends on a few substitutions, permutations and direct changes. It said that up until today, no functional assault against AES exists. In this manner, governments, banks and high-security frameworks around the globe are favored utilizing AES for the encryption standard. [13]. It is highly securable and more efficient algorithm and it secure all types of data that deals with medical information‘s but only thing need for more design area. Here AES algorithm is used that consists of 22 rounds it may minimize to 18 rounds which reduce time consuming and cost [14]. The use of AES encryption algorithm is highly securable with no loopholes and AES encryption and decryption is highly secured and fastest method. AES is the main algorithm which is not inclined to any of the cryptanalysis assaults (attacks). [15].

### 4.2 Asymmetric Techniques

#### 4.2.1 RSA

Ronald Rivest Adi Shamir and Leonard Adleman designed the RSA algorithm 1977 cryptosystem uses the properties of the generative homomorphism encryption. RSA key size is having 1024 bit. Then its have one rounds [8]. RSA is generally use public key techniques and RSA is accomplished to maintain encryption and digital signatures. RSA provides the best security plan by encrypting the data that is confidential; this is the motivation behind why the enormous administration suppliers like Google mail, Yahoo mail and so on are utilizing this algorithm to give their clients the protection of secrecy in utilizing their administrations [13].RSA today is utilized as a part of a few programming items and it can be utilized for digital signatures, key exchange, or encryption of a little block of data. RSA uses a changeable size key and a variable size encryption block but RSA encrypts and decrypts data that consumes more time [10].

#### 4.2.2 DSA

In presented an autonomous investigation of security algorithms in cloud computing. Which provides the particular technique to secure data on cloud computing. The DSA technique gives digital signature possibilities for the authentication of messages [10] DSA (Digital Signature Algorithm) is a Federal data processing Standard for digital signatures. DSA was introduced by the NIST (National Institute of Standards and Technology) it is used to detect the unauthorized alterations to the data send by the source to the receiver [8].

#### 4.2.3 Diffie-Hellman

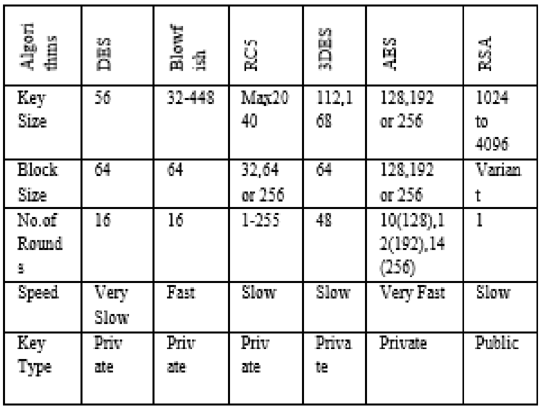
Diffie-Hellman introduces secret-key exchange protocol only. It is not for authentication or digital signatures and it is public key exchange methods, it uses of the discrete logarithm problem. Actually the sender and receiver set the secret key [10]. These techniques protect the data confidentiality and safe and security, Diffie Hellman Key Exchange method to link organization and Elliptic curve cryptography for data encryption [16].

#### 4.3.4 El-Gamal

El-Gamal algorithm is also public key cryptographic techniques. The private key will be secret. It is not capable to expose the information. So encryption and decryption of message will gives more security for the data, EL-Gamal's cryptosystems have numerous helpful applications, with its strong properties. It is an exceptional sec. This is most certainly not restrictively difficult to encrypt the message in the cloud also [17]. The unique data is then acquired by the user with the cipher Keys. This must be reached out for a various number of clouds and with various operations. [18].

## VI. Comparison of Symmetric and Asymmetric Algorithms

**Table 1.** Comparison of Symmetric and Asymmetric techniques



| Algorithms | DES | Blowfish | RC5 | 3DES | AES | RSA |
|---|---|---|---|---|---|---|
| Key Size | 56 | 32-448 | Max2040 | 112,168 | 128,192 or 256 | 1024 to 4096 |
| Block Size | 64 | 64 | 32,64 or 256 | 64 | 128,192 or 256 | Variant |
| No.of Rounds | 16 | 16 | 1-255 | 48 | 10(128),12(192),14(256) | 1 |
| Speed | Very Slow | Fast | Slow | Slow | Very Fast | Slow |
| Key Type | Private | Private | Private | Private | Private | Public |

## VII. CONCLUSION

The paper concludes with an independent study of security algorithms in cloud computing such as symmetric, asymmetric techniques. The symmetric and asymmetric techniques such as DES, Blowfish, RC5, 3DES, AES, RSA, DES, Diffie-Hellman and ElGamal. The study says that on comparison with many secured algorithms available till date, blowfish is faster than other encryption algorithms. AES algorithm uses least time to execute cloud data. DES algorithm consumes least encryption time. RSA consumes longest memory size and encryption time and other algorithms are very slow.

## VIII. REFERENCES

[1]. Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", IJETAE, Volume 3, Issue 12, December 2013.

[2]. AbhinayB. Angadi, Akshata B. Angadi, Karuna C. Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", IJARCET, Volume 2, Issue 2, February 2013.

[3]. A. N. Suresh, Ch. Sailaja, G. Gayatri, D.V.S. Deepak, "Security Challenges In Cloud Computing", IJERT, Vol. 2 Issue 2, February-2013.

[4]. Dr.Nedhal A. Al-Saiyd, Nada Sail, "Data Integrity in Cloud Computing Security", Journal of Theoretical and Applied Information Technology, 31st December 2013. Vol. 58 No.3

[5]. Rushikesh Vilas Belamkar, "Challenges and Security Issues in Cloud Computing", ISRJ, ISSN 2230-7850, Volume-4, Issue-2, March-2014.

[6]. RandeepKaur, SupriyaKinger.2014Analysis of Security Algorithms in Cloud Computing. International Journal of Application or Innovation in Engineering & Management 3: 171–176.

[7]. SunithaSharma et al.2013Enhancing Data Security In Cloud Storage. International Journal of Advanced Research in Computer and Communication Engineering, 2: 2132–2134.

[8]. Nikhitha K, Navin K S.2015A Survey On Various Encryption Techniques For Enhancing Data Security In Cloud. International Journal of Advanced Research Trends in Engineering and Technology 194– 197.

[9]. Vijendra et al.2014Data Storage Security in Cloud Environment with Encryption and Cryptographic Techniques. International Journal of Application or Innovation in Engineering & Management, 3: 209–213.

[10]. CharanjeetKaur et al.2015Data Security Algorithms In Cloud Computing: A Review. International Journal For Technological Research In Engineering 2:372– 375.

[11]. Jay Singh et al.2012Improving Stored Data Security In Cloud Using RC5 Algorithm. Nirma University International Conference on Engineering. pp. 1–5.

[12]. DeepikaVerma, Karan Mahajan.2014To Enhance Data Security in Cloud Computing Using Combination of Encryption Algorithms, 2: 41–44.

[13]. Nasrin K, ZurinaMohd.2014A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services. IEEE Conference on Systems, process and Control pp. 58-62.

[14]. SaiSindhuTheja R et al.2015Data Security in Cloud for Medical Sciences using AES 512-bit Algorithm. International Journal on Recent and Innovation Trends in Computing and Communication 1746– 1749.

[15]. LovepreetKaur et al.2015A Survey on the Encryption Algorithms in the Cloud Security Applications. International journal of Science Technology & Management (IJSTM), pp.1– 9.

[16]. Honey Patel, JasminJha.2012Securing Data in Cloud Using Homomorphic Encryption. International Journal of Science and Research. 4, :1892–1895.

[17]. Jayanthi M et al.2014Analysis on Secure Data Sharing using ELGamal‘s Cryptosystem in Cloud. International Journal of Computer Science and Electronics Engineering, 4:50–55.

[18]. Raghul et al.2015Data Security in Federated Cloud Environment using Homomorphic Encryption Technique. International Journal of Emerging Technology and Advanced Engineering, 5:137–141.

[19]. Sana Belguith et al.2015Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm. The Eleventh International Conference On Autonomic and Systems. 98– 103.

[20]. Tembhurne S et al.2015An Improvement In Cloud Data Security That Uses Data Mining. International Journal of Advanced Research in Computer Engineering & Technology 4: 2044–2049.

[21]. NiteenSurv et al. Framework for Client Side AES Encryption Techniques in Cloud Computing. International Advance Computing Conference (IACC), 525– 528.

[22]. Pradeep Kumar et al2014An authentication approaches for data sharing in cloud environment for dynamic group. International conferences on issues and challenges in intelligent computing techniques (ICICT) 9:262–267.

[23]. Rashmi S et al.2015Architecture for Data Security in Multi-cloud Using AES-256 Encryption Algorithm. International Journal on Recent and Innovation Trends in Computing and Communication 157-161.

[24]. Masthanamma V et al.2015An Efficient Data Security in Cloud Computing Using the RSA Encryption Process Algorithm. International Journal of Innovation Research in Science, Engineering and Technology 4: 1441– 1445.

[25]. Anuj Kumar et al.2014Cloud Data Security using Authentication and Encryption Technique. International Journal of Innovative Research In Technology 1: 388– 391

[26]. Prashantrewagad et al.2013Use of digital signature with Diffie Hellman key Exchange and AES encryption algorithm to enhanced data security in cloud computing. International conference on communication systems and network technologies. 3:437-439.

[27]. Sonia sindhu.2015A survey of security algorithms in cloud computing. International journal of Advanced Research in Computer Engineering & Technology,