A Review Paper of Data Security in Cloud Computing

Ravikant Gupta¹ & Dr. Ravikant Kapoor²

¹ Research Scholar, Department of Computer Engineering and Application, NITTTR Bhopal, India
² Associate Professor, Department of Computer Engineering and Application, NITTTR Bhopal, India

Abstract: Cloud computing has its promising future because of features provided by it. Since cloud computing is network based technology, it requires security attention. Researchers have contributed a lot in this specific area and proposed many algorithms like AES, Blowfish, DES under symmetric key and RSA and Diffie-Hellman under asymmetric. These algorithm proposed by authors and researchers have their own advantages and disadvantages. Purpose of this paper is to do exhaustive survey to find out research gap and challenges for suggesting a feasible solution with a new approach and to set future research direction.

1. Introduction

In this era of digitization, an organization or individuals may require to have huge storage banks to store their valuable data which may be a costly and complex affair for them. With the Cloud computing and storage solutions it is possible for users and enterprises to have verity of solutions with various capabilities to store and process their data at the third-party data centers. In this way Organizations come across with Cloud in a variety of different service models (SaaS, PaaS, and IaaS). With cloud computing, there are number of security concerns associated. These issues fall into two broad categories:

(1) Security issues faced by cloud service providers (organizations providing software as a service, platform as a service or infrastructure as a service via the cloud) and

(2) Security issues faced by the customers (companies or organizations who utilize the applications or store data on the cloud).

However, In order to provide reliable services, the cloud service provider must ensure the security of their infrastructure and that their clients’ data and applications are protected and remain integrated. At the same time the user must take measures to strengthen their application and use strong passwords and authentication techniques.

Research community has found out some security and privacy issues in the cloud computing.

Fig1. shows the hierarchy of analysis of security in cloud computing. This describes the cloud, cloud service model and depicts that each service model have many security challenges/issues. For example Software as a Service model has data security, data locality, data segregation, data access, web application security and other problems. These security problems and threats are solve by many security techniques such as identity and access management guidance, dynamic credentials, digital signatures, homomorphic encryption, encryption, web application scanners, Hypersafe, mirage etc. Data security is fundamentally based on three principles such as CIA (Confidentiality, Integrity, and Availability). Here many researchers advocate that confidentiality is an essential principle of data security in cloud computing for users to store the confidential data and private message. Secure communication and secure data transition is only possible through cryptography. Cryptography is a process for converting the actual data as a plane text to encrypted data as a cipher text and vice versa.

Data converting process is also called the Encryption and Decryption technique. Encryption / Decryption cryptographic techniques are categorized into three algorithms such as Symmetric key algorithm, Asymmetric key algorithm and hash function. In this hierarchical chart the last level is to describe the asymmetric key algorithms that work with two different keys, a public key for encryption and a private key for decryption.
Figure 1. Narrow down the chart of Analysis of Security in Cloud Computing.

The research community has proposed many solutions in the area of data security in cloud computing. Major work carried out by them is discussed in next section.

2. Literature Review

R.Velummadhava Rao et al. [9] have focused on security issues and its solutions through the encryption techniques. They suggest a data security model comprises of authentication, data encryption, data integrity, data recovery and user protection has to be designed to improve the data security over cloud. And also suggest before the data is stored and transmit to the cloud server, data encryption should be necessary. In cloud computing, RSA based data integrity check can be provided by combining identity based cryptography and RSA signature. To compute large files with different sizes and to address remote data security RSA based storage security method can be used.

Rakhi Emelaya et al. [10] mentions that different types of encryption techniques such as AES, Blowfish, RC4, RSA, KB-ABE, and hashing algorithms such as MD5, SHA-1, 2, 3 are provided to enhance the performance, encryption time and decryption time. Here it is also focused that blowfish algorithm give a better performance and more security and strongest against any type of intrusion.

An optimized blowfish has been developed the longer key size is more secure but the encryption time and decryption time is slow. In order to overcome this problem in blowfish algorithm reducing of two S-boxes will increase the speed and provide the better security to data.

Shakeeba S. Khan et al. [11] have proposed multilevel encryption and decryption to provide security for cloud computing storage data with the help of RSA and DES algorithms rather than single level encryption and decryption. DES implements the first level of encryption and that encryption to use by RSA and RSA implements the second level of encryption or vice versa. They suggest existing cryptographic algorithms are single level encryption algorithms that are not safe for cyber criminals. Cyber criminals can easily cracked single level encryption. So we can use multilevel encryption and decryption to provide more security for cloud storage.

Dr. S. Gunasekaran et al. [12] have focused on a review of cryptographic algorithms such as AES, RSA, and MD5. It is found that RSA and AES both are better than others for enhancing the data security in cloud computing.

S. Hemalatha et al. [13] have introduced for security strength of RSA and Attribute based encryption for data security in cloud computing. RSA and ABE encryption algorithms are compared based on the key pairing based cryptographic algorithm and integer factorization cryptography. Here Key size is play a vital role because to some extent it eliminates the element of cryptanalysis. So if we increase the key strength than data is more secure.

Vanya Diwan et al. [5] have compared different cryptographic algorithms such as DES, AES, RSA and ECC based on the key length, block size, security rate, execution time and AES & RSA better than to other. Here focused that on different data files those are stored in cloud server. File can be uploaded in encrypted form and can be downloaded with the help of key. They suggest if we use encryption and decryption process in uploading and downloading data than IT companies can benefit a lot from cloud computing as all the data can be centralized in a protective environment.

Balkees Mohamed Shereek et al. [14] have proposed the RSA encryption with Fermat’s Little Theorem that is reduced the key generation time when we select the large key size for encryption and decryption process.

Jashanpreet Pal Kaur et al. [7] have focused the security issues and its solutions with the help of
cryptographic algorithms such as symmetric, asymmetric and hash function and also compared to each other for concluding the which one is better using with different parameters and suggest us if we combine these (symmetric, asymmetric and hash) algorithms than that will too complex in term of computational efficiency.

Rachna Arora et al. [15] have focused on many encryption algorithms such as AES, Blowfish, DES, RSA and compared with its characteristics and also decide the which one is better. AES algorithm takes least time to execute data. Blowfish algorithm has least memory requirement. DES algorithm consumes least encryption time. RSA takes longest memory size and encryption time.

Rashmi Nigoti et al. [8] have described symmetric (such as DES, 3-DES, AES and Blowfish) and asymmetric algorithms (such as RSA, Diffie-Hellman key exchange). DES and AES are mostly used for symmetric algorithms. DES is better than AES in the case of implementation. In cloud computing, RSA and Diffie-Hellman Key Exchange are used to generate the encryption keys for symmetric algorithms. Security algorithms will maintain the confidentiality of data.

Swadeep Singh et al. [16] have compared between ECC and RSA algorithms. This paper also says that RSA are comparatively faster than ECC. In RSA algorithm, encryption and key generation are faster whereas decryption is slower. In ECC algorithm, key generation and encryption are slower whereas the decryption is faster.

Dr. Prena Mahajan et al. [17] have focused on encryption algorithms like AES, DES and RSA. If we take the text files and concludes the experimental result than AES algorithm consumes least encryption and RSA consumes large encryption time. Decryption of DES algorithm is better than other cryptography algorithms.

B. Padmavathi et al. [18] have proposed the existing encryption algorithms such as AES, DES, and RSA with LSB substitution technique and compared each other. Based on the experimental result it was concluded that AES algorithm takes less time for encryption, decryption and buffer usage time as compared to DES algorithm. But RSA consumes more encryption time and buffer usage is very high. Finally observed that AES algorithm is better than DES and RSA algorithms.

Main Title
The main title (on the first page) should begin 1-3/8 inches (3.49 cm) from the top edge of the page, centered, and in Times 14-point, boldface type. Capitalize the first letter of nouns, pronouns, verbs, adjectives, and adverbs; do not capitalize articles, coordinate conjunctions, or prepositions (unless the title begins with such a word). Leave two blank lines after the title.

3. Research Challenge
In this study we have found some research gap and challenge which are still to be resolved. Mainly the Researchers have done work related to symmetric and asymmetric cryptographic algorithms used for encrypting and decrypting the data. But every encryption algorithm has some limitation such as key generation, block size of data, key length, and encryption/decryption conversion time etc. symmetric algorithms and hash function both are faster than asymmetric algorithms in terms of computation speed but a big problem of key agreement/exchange in symmetric algorithms are that they are easily breakable as compared to asymmetric algorithms. Asymmetric algorithms are more secure as compared to symmetric algorithms based on the key exchange. So finally RSA algorithm is more valuable in asymmetric algorithms. But RSA consumes more encryption/decryption time and its buffer usage is very high. RSA also involves more mathematical calculations for encrypting and decrypting data/message thus the data is more secure.

4. Conclusion
In the era of cloud computing, security is a major issue for all communication and transaction to store and retrieve the data on cloud storage server. Security is only possible with the help of cryptographic algorithms; either we use symmetric or asymmetric algorithms. This paper describes all major cryptographic algorithms and their comparison that gives the best solution which algorithm is better than other algorithms based on some specific parameters. Now a day, many researchers proposed many models and algorithms for security purpose but they compare the algorithm or model with the RSA. So RSA can be considered as very popular and secure for data transmission in cloud computing. RSA algorithm has not only been singly used, but also as a hybrid cryptosystem [19] [20] i.e. a combination of symmetric and asymmetric algorithms.

5. Future Research Direction
Type It is identified that almost every researcher used asymmetric algorithms a special case for RSA because RSA and Diffie-Hellman key exchange is used to generate encryption keys for symmetric algorithms. So we are focusing here only for RSA
asymmetric algorithm that has some limitations such as encryption/decryption time, key length, block size, mathematical calculation, more complex etc these limitations we can attempt to improve with the help of key generation encryption algorithms (KGEA) such as 2KGEA/ 3KGEA /5KGEA [21] [22] and also increase the key strength for generating the least encryption and decryption time.

6. References