International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 10 | Oct -2020 ISSN: 2582-3930

# A Review on Various Algorithm for Data Security and Privacy in Cloud Computing.

**Renuka S. Durge[1], Vaishali H. Deshmukh[2]**

*[1]Renuka S. Durge, Computer Science & Engineeering*
*[2] Vaishali H. Deshmukh, Computer Science & Engineeering*

## Abstract

Cloud computing has now become a major trend; it is a new data hosting technology that is very popular in recent years. Cloud computing is one of the most emerging technologies which plays an important role in the next generation architecture of IT Enterprise. It has been widely accepted due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry As the development of cloud computing, security issue has become a top priority. The challenges in privacy protection are sharing data while protecting personal information.. In this paper we present the major security issues in cloud computing and we also propose a simple, secure, and privacy-preserving. Cloud data sharing based on an encryption/decryption algorithm which aims to protect the data stored in the cloud from the unauthorized access. Security of data in cloud is one of the major issue which is more complication in the implementation of cloud computing. These security issues are avoided by various encryption algorithms.

***Keywords*** *: Cloud computing, Encryption, Algorithm, Cryptography.*

## 1. Introduction

Cloud computing has gained substantial research interest, owing to its vast range of services. The major issues in cloud computing are its security and privacy. The term security has multiple facets such as confidentiality, availability and integrity. A perfect security solution must ensure all the security parameters effectively. Thus focuses on the security of data alone.

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. So we make a comparative research analysis of the

existing research work regarding the data security and privacy protection techniques used in the cloud computing.[1]

Data security is a common concern to all technologies. However, it becomes a major challenge when applied to an uncontrolled environment like Cloud Computing. Data storage is distributed over a number of Datacenters around the world. Data calculation is carried out by virtual machines. Users can create different virtual machines, with different capacities and numbers to suit their needs [2]. The transfer of data calculation and storage to a third party involves the transfer of responsibility associated with their security and compliance to this third party .The calculation in the Cloud takes place as follows: the user first submits his data to the datacenter that is stored and managed by storage service. This data is then sent to the virtual machines for parallel processing using the corresponding distributed technology. After the end of processing, users can download and view the results. During this process, all private or confidential data may be disclosed.

Based on this process, we can distinguish three states relating to the data in the Cloud: data-at-rest, i.e. the data stored, data-in-transit i.e. the data transmitted and the data-in-use i.e. data accessed or being processed. Therefore, data security and exploitation in the Cloud must cover these three aspects. At each stage of this data life cycle, different measures can be implemented to ensure data security. We highlight in this section the data security issues related to each stages of this life cycle. These issues have been extracted from various paper dealing with the subject.

i. Data-at-rest Data storage is one of the most commonly used services in the Cloud. It offers the user an “unlimited” space and allows him to access his data ubiquitously at a lower cost. Data-at-rest security refers to securing data on the storage media. It is difficult to achieve for the user due his limited physical control over the data. [3].

ii. Data-in-transit Data-in-transit security refers to the security of data transmissions in the Cloud. It ensures that the data will not be intercepted, altered or replaced. data-in-transit can be very sensitive like user names and passwords. Data-in-transit may be more at risk than data-at-rest, as they travel from one place to another [4].

iii. Data-in-use refers to any reading or processing (creation, transformation or deletion) of data. When processing take place in the Cloud, the risks of misuse increase, due to the large number of users involved in Cloud. In a traditional environment, the user holds, and manages his data. However, in Cloud Computing a user’s data can be generated and handled by a third party. The problem for the owner is to keep control over his data created by another. For personal and private information, the owner must know what personal information is collected, and in some cases, stop collecting and using of this information. Furthermore, Owners of data need to ensure that the use of their data is consistent with the purposes of the collection and that private information is not disclosed to third parties [5].

**Table 1. Review on various Research Papers on Data security using different algorithm.**

| Sr.no | Author | Paper | Method | Advantages | Disadvantages |
|---|---|---|---|---|---|
| 1. | Noha MM. AbdElnapi. April 2016 [10] | A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing | Combination of RSA ,AES and Hybrid hash Function | Performance has increase by hybrid encryption | Time of execution is more than encryption algorithm of RSA & AES. |
| 2. | Zaid Kartit January 2016 [13] | Applying Encryption Algorithm for Data Security in Cloud Storage | Homomorphic encryption For uploading and downloading files. | Algorithm technique works fast in both directions upload and download | Efficiency is lacking |
| 3 | Sheenal Malviya, Nov 2018 [16] | Secure Data Sharing Scheme using Cryptographic Algorithm for Cloud Storage | Paillier algorithm is suitable for numerical data encryption | provide a dynamically secure group data sharing and access services in a decentralized manner. | Doesn't work for text based cryptography |
| 4. | P Varaprasada Rao May 2019 [18] | Improve the Integrity of Data Using Hashing Algorithm | Comparative study on all hash function. | MD5 hash function is more faster, No reverse process can be done. | hash for a password is generated it is stored in a database |

## 2. Related Work

Data Encryption (Cryptographic) Algorithm may be of three types[8] :

i) Symmetric or Secret Key Cryptography In this kind of cryptography for both encryption and decryption a single key is used. And same key should be known to both sender who encrypts the message and the receiver who decrypts. DES, Triple DES, AES, RC5, etc may be the example of such encryption.

ii) Asymmetric or Public Key Cryptography Different key is used for both encryption and decryption in this cryptographic algorithm. Message sender encrypts the message or data using public key that may be known to all publicly. On the other side message receiver uses other secret key to decrypt the message. In this cryptography both public and private key can be used only for one purpose. RSA, Elliptic Curve, etc may be the examples of such Encryption.

iii) Hash Function In this cryptography no key is used and only some mathematical methods are used. Data cannot be decrypted back to plain text after encryption in this algorithm. So it also can be known as one-way encryption.

Hashing algorithms are just as abundant as encryption algorithms, but there are a few that are used more often than others. Some common hashing algorithms include MD5, SHA-1, SHA-2, NTLM, and LANMAN.

*MD5*: This is the fifth version of the Message Digest algorithm. MD5 creates 128-bit outputs. MD5 was a very commonly used hashing algorithm. That was until weaknesses in the algorithm started to surface. Most of these weaknesses manifested themselves as collisions. Because of this, MD5 began to be phased out.

*SHA-1*: This is the second version of the Secure Hash Algorithm standard, SHA-0 being the first. SHA-1 creates 160-bit outputs. SHA-1 is one of the main

algorithms that began to replace MD5, after vulnerabilities were found. SHA-1 gained widespread use and acceptance. SHA-1 was actually designated as a FIPS 140 compliant hashing algorithm.

*SHA-2*: This is actually a suite of hashing algorithms. The suite contains SHA-224,

SHA-256, SHA-384, and SHA-512. Each algorithm is represented by the length of its output. SHA-2 algorithms are more secure than SHA-1 algorithms, but SHA-2 has not gained widespread use.

*LANMAN*: Microsoft LANMAN is the Microsoft LAN Manager hashing algorithm. LANMAN was used by legacy Windows systems to store passwords. LANMAN used DES algorithms to create the hash. The problem is that LANMAN's implementation of the DES algorithm isn't very secure, and therefore, LANMAN is susceptible to brute force attacks. LANMAN password hashes can actually be cracked in just a few hours. Microsoft no longer uses LANMAN as the default storage mechanism. It is available, but is no longer turned on by default.

*NTLM*: This is the NT LAN Manager algorithm. The NTLM algorithm is used for password hashing during authentication. It is the successor of the LANMAN algorithm. NTLM was followed with NTLMv2. NTLMv2 uses an HMAC-MD5 algorithm for hashing.

## 3. Proposed work

The main contribution of the proposed work will be in terms of encrypting data of the cloud is that the algorithm can encrypt up to 192 bits of data at a time. So in cases of encrypting a large amount of data the algorithm works efficiently saving more time. Each of the rounds and the algorithm itself has been designed in such a way that it is impossible to crack or decipher the encrypted texts without the key. Each round of encryption and decryption process has several customize permutation which makes the algorithm more secure from theft. By using a secure encryption and decryption process and a large key size of 192 bits and secure using as hash function, the proposed algorithm achieves the cryptographic goals which are confidentiality, integrity and authentication. So it provides robust security to the data stored in cloud for which it has been designed for.

## 4. Conclusion:

Although Cloud storage has many advantages; there are still many actual problems concerning security that need to be solved. If we can eliminate or master this weakness of security; the future is going to be Cloud storage solutions for large as well as small companies. In this research we are going to present the different vulnerabilities related to cloud computing, we have also proposed a solution to improve the security of the storage of data, data security is provided by implementing our algorithm. Only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data, he can't decrypt it. The goal of the proposed algorithm is to secure and enhance the protection of data stored in cloud.

## References:

[1] Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing.In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5.IEEE (2016)

[2] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4, 5 (2013).

[3] Kulkarni, G., Gambhi, J., Patil, T., Dongare, A.: A security aspects in cloud computing. In: IEEE 3rd International Conference on Software Engineering and Service Science, pp. 547–550. IEEE (2012)

[4] Mahmood, Z.: Data location and security issues in cloud computing. In: IEEE International Conference on Emerging Intelligent Data and Web Technologies, pp. 49–54. IEEE (2011)

[5] Roy, N., Jain, R.: Cloud computing: architecture and concept of virtualization. J. Sci.Technol. Manag. 4 (2015). 2394-1537

[6] Ankid Fadia, Jaya Bhattacharjee, "Encryption, Protecting Your Data", Vikash Publishing House Pvt Ltd,2007, ISBN: 812592251-2

[7] Paul C. Kocher, "Timing Attacks on Implementations of DiffeHellman, RSA, DSS, and Other Systems", Cryptography Research Inc., San Francisco, USA.

[8] Alongbar Daimary "A Study of Different Data Encryption Algorithms at Security Level: A Literature Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3507-3509.

[9] Kulkarni, G., Gambhi, J., Patil, T., Dongare, A.: A security aspects in cloud computing. In: IEEE 3rd International Conference on Software Engineering and Service Science, pp. 547– 550. IEEE (2012).

[10] Noha MM. AbdElnapi. "A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing"., International Journal of Computer Science and Information Security, Vol. 14 (4) , April 2016.

[11] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4, 5 (2013).

[12] Roy, N., Jain, R.: Cloud computing: architecture and concept of virtualization. J. Sci. Technol. Manag. 4 (2015). 2394-1537.

[13] Zaid Kartit "Applying Encryption Algorithm for Data Security in Cloud Storage" https://www.researchgate.net/publication/301324486. ,January 2016.

[14] Sudhansu Ranjan Lenka "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014.

[15] Kaleem Ur Rehman, "HASH CODE BASED SECURITY IN CLOUD COMPUTING" International Journal of Advanced Technology in Engineering and

Science www.ijates.com Volume No.02, Issue No. 06, June 2014.

[16] Sheenal Malviya "Secure Data Sharing Scheme using Cryptographic Algorithm for Cloud Storage "International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 20 (2018) pp. 14799-14805.

[17] Saidhbi Sheik " A Way to Secure the Data in Cloud Data Storage by Using Cloud Data Compression Mechanism" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018.

[18] P Varaprasada Rao, " Improve the Integrity of Data Using Hashing Algorithms" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, May, 2019.