International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Cryptographic Solutions for Cloud-Based Storage System

Anuj Kumar Yadav, M.L.Garg, Ritika

Abstract: ***Nowadays cloud computing is a driving force which has a large impact on each aspect of our lives and widely used in today's business structure. With its capacity and capability, it is widely accepted by many organizations and users. Cloud computing provides numerous benefits to end users and companies in terms of cost, maintenance, management due to which many organizations prefer to use its services with open hands. With the increasing demand, day-by-day service providers also increased and the user has a choice to choose the best one based on their demand Cloud Storage is one such service that provides cost effective storage solution to the users. They provide unlimited storage to the users based on the requirement and charge according to that only. User can rely on them for the storage but apart from the numerous benefits security and privacy remains the biggest concern whenever a user moves to cloud services. Security triad comprises of authentication, Integrity, and availability remains the concern for every user while moving towards cloud-based services. Almost everyday industry and academician working on finding an effective and efficient way, which could provide secure migration of user data in the cloud. One of the solutions could be the use of cryptographic techniques to provide data security. Cryptography is accepted largely to ensure the privacy and security of data in cloud computing. In this paper, several cryptographic technique discussed which are expected to provide the solution to the user's problem when they tend to move towards cloud computing.***

Index Terms: ***Cloud Storage, AES, Blowfish, DES, Diffie Hellman, RSA.***

I. INTRODUCTION

In recent years our society related to information technology have been benefitted by a new buzzword known as cloud computing. The term is associated with almost every field and due to its large benefits, it is also widely accepted to different categories of users. We can say it is a prime drive force in today's IT world. Cloud computing generally perform the work on a variety of platforms like mobiles, computers, laptops, etc. the basic requirement is only the availability of working internet connection. The cloud user pays for used IT services provided by the cloud service provider. There are varieties of services provided to users based on the requirement in a very cost-effective manner. User can be categories as individuals, academician, government organizations, IT industry, etc. All these organizations get the services either in the form of software, platform or infrastructure [1].

The core technology behind the cloud computing is virtualization. With virtualization, cloud services and resources can be divided into logical manner [2]. Cloud services are not limited to above-mentioned services but users can also use cloud computing or cloud storage to store their data in an efficient manner. When compared to the traditional storage system, cloud storage provides various benefits to the end user. The factors on which the benefits evaluated comprises of capacity, scalability, accessibility, data recovery, cost, etc. Apart from all the benefits and advantages, data always reside outside the user's premise due to which user always thinks whether the data is secure or not at the cloud server.

The issues related to the cloud can broadly classified into two categories. First, issues faced by cloud customers and second issue faced by the cloud service provider. In this paper, we are considering the issues of security for the cloud end user. From the end user's point of view, risk is largely associated with uploading and sharing the file [3].

In the paper, we will discuss all the factors regarding the cloud storage and find out the solution to the problem, by which the user can be benefitted. The paper is divided as follows: In section 2 cloud storage is defined with its benefits, In section 3 several cryptographic algorithms are discussed in brief, In Section 4 all these algorithms are compared on various factors and Finally in section 5 paper concludes.

II. CLOUD STORAGE

Cloud computing has largely associated with each aspect of our life and cloud storage is one of the aspects [4]. There are various ways in which we can define the term cloud storage, some of them are as follows:

- In cloud storage data is stored, managed and maintained at the remote location. Cloud storage provides the facility to users, using which user can store a file at a remote server. By storing, the file at remote server user can access the file from anywhere using the internet connection [5].Cloud storage can be viewed as

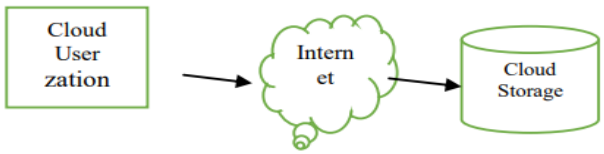

Figure 1: Cloud Storage

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
Anuj Kumar Yadav, CSE, DIT University, Dehradun, India.
Dr M.L. Garg, CSE, DIT University, Dehradun, India.
Dr Ritika, MCA, DIT University, Dehradun, India.

- Cloud storage can be defined in two parts as. First part is related to the services that provides application model to the user using which user can connect to the cloud storage using the network and save data in the cloud storage round the clock. The second part is related to build up of storage services. By this build up, the user achieves low power, cost-effective shared storage space which can be used by the user to achieve various tasks [6].
- Cloud storage can be view as a storage space for files, where files are stored online in the cloud. In place of using traditional ways(local HDD, External HDD, Flash Drive) for storing the files, the user can save their files online. By using this approach user can access the files from any internet-enabled device such as a mobile, tablet or any other computing device [7][8].

Apart from the above-mentioned definition, there are different ways in which we can define cloud storage. Cloud Storage provides various benefits to end users, some of them are as follows:

A. Benefits of Cloud Storage:

World Wide accessibility: The prominent advantage of using cloud storage is the accessibility of data from anywhere. User need not carry and storage device to get access to his or her data.

Ease in data sharing: User can share his data with ease to any no of users in a secure manner as only authenticated users get access to the data [9].

Storage space saving: With the help of cloud storage user can reduce the memory requirement of their system and saves the storage space of HDD.

Scalability: All the cloud storage service providers, facilitate the users with the advantage of choosing the storage capacity on demand. User can scale up or scale down his storage requirement in run time or dynamically.

Cost Effective: All the cloud storage service provider generally charge according to the usage, even some service providers, gives free storage space but it's limited to a few GB of data. So user need not purchase storage space at a large cost, he or she can pay for storage according to the usage.

Minimal data maintenance: User or administrator need not keep track of their data, as data is to maintain and managed by the cloud service provider [10].

All of the above said benefits provided to the user when they use cloud-based storage from various available cloud service providers. Some of the major cloud storage providers are as follows:

- Amazon Drive: It provides 5 Gb free cloud space for storage and user have to pay for extra space.
- Google Drive: It provides 15 Gb storage space to its users which user can use to store a variety of documents, photos, and other files. User can upgrade to Google One any time for more space and have to pay according to the additional space.
- Microsoft OneDrive: This is the cloud storage service provided by Microsoft's. Here user gets 5 Gb free space to store a different kind of files.
- Apple iCloud: This is the cloud storage service provided by Apple's that's available to any Apple user, whether a user has an iphone, iPod, or Mac>% Gb space is free to use but user have to pay for extra storage space.
- Dropbox: It is one of the mostly use cloud storage application that provides 2 Gb of free space to the users. The user can purchase an enhanced version called Dropbox Plus if space requirement is more than 1 TB [11].

Apart from the benefits listed above, there are some limitations and issues that are associated with the cloud-based storage systems. Some of them are as follows:

- **Dependency On Network availability:** As mentioned earlier cloud-based solutions heavily rely on the speed of internet connection, having low speed can hamper the data accessing in real time. Apart from this, there are some remote areas where internet connection availability is not up to the mark or even not available.
- **Issue related to privacy:** While using cloud storage, the user always concerned about their data. User does not know who is maintain and managing the data whether it is a client, server, company or storage network [12].
- **Possibility of Data Loss:** If a user opts out of using the cloud storage before the actual contract ends, the user needs to fulfill all the mandatory requirements regarding payment, etc otherwise early termination may lead to data loss [13].

So On the basis of discussed points, we can say cloud storage provides cost-effective storage solution but when it comes to the security, there are always some concerns from the user point of view that is why a user may hesitate to opt for a cloud-based storage solution. In addition, when a normal user changes its storage service from local disk to cloud storage, it can be stress full for the user [14].

III. SECURITY ALGORITHMS FOR CLOUD STORAGE:

The data stored in the cloud should be secured from a user point of view and only the valid users should access the data. Cloud storage is situated at remote locations that are unknown to the end user. To provide security to such data is an uphill task and this required many efforts. To provide a solution to such problem, cryptography provides a variety of algorithms. These algorithms provide the data security as they convert the original data (plain text) into coded form (cipher text) and coded form data is transferred through the communication channel and only authenticated users can access that data. In this paper, some of the cryptographic algorithms are explained about how they are converting normal text to the coded form [15]. All these algorithms have certain evaluation parameters based upon which the performance of these algorithms is measured.

Some of the widely used performance parameters are plain text size, block size, key size, etc. Cryptographic algorithms can be categorized into two types

- Symmetric key cryptographic algorithms
- Asymmetric key cryptographic algorithms

A. *Symmetric key cryptographic algorithms*

These algorithms are also called secret key algorithms, in which communicating parties share the same key for encryption and decryption. The key needs to keep secret by both sender and receiver if the condition got violated attacker can steal the data during the transmission. There are many algorithms of symmetric key cryptography; some of the algorithms are DES, AES, IDEA, DOUBLE DES, TRIPLE DES, Blowfish, etc. Few of them are as follows :

- **DES**

DES algorithm is based on Fiestal Structure. DES is block cipher in which plaintext of 64 bits is converted into a cipher text of 16 bits. DES performs the desired operation in 16 rounds and key used is of 56 bits (original size is 64 bits but every eighth bit is discarded to disguise the attacker). Algorithms provide desired result after completion of 16 rounds [16].

- **Double DES and Triple DES**

Both Double and Triple DES are an extension of DES algorithm. In double DES two keys are used from encryption and decryption. In triple DES block size used is of 64 bits with the key length of 56 bits. It performs DES operation three times on each block of data. Triple DES uses 64 bits plaintext with 48 rounds and a key length of 168 bits [17].

AES: There was some limitation of DES, and to overcome these limitations AES was introduced. AES is also asymmetric key-based block cipher algorithm and it is a widely used algorithm for data encryption. In AES there are 3 versions named as AES-128, AES-192, and AES-256. AES-128 encrypts, decrypt data block of 128 bit, AES-192 encrypts, and decrypt data block of 192 bit and AES-256 encrypts and decrypt data block of 256 bit [18].No. of rounds of each version varies and comparison is shown in the table 1 given below:

Table 1: AES Versions

AES Version	No. of Rounds
AES-128	10
AES-192	12
AES-256	14

Blowfish Encryption Algorithm: It is one of the most efficient algorithms of symmetric key cryptography in which variable length key is used. The key length can have length up to 448 bits. The algorithm uses a block size of 64 bits. The algorithm performs desired operations in two phases. In the first phase key expansion performed, in which 448-bit key expanded into subkeys. In the second phase, the encryption performed. The algorithm is widely used in password management systems, bitmap image plotting, etc [19].

B. *Asymmetric key cryptographic algorithms*

These algorithms are also called public key algorithms, in which communicating parties have different keys. The keys used for encryption and decryption are public and private keys. Public keys are distribute to communicating parties using various methods and private keys is kept secret with the user. For encryption and decryption both of the keys are required as a pair. There are many algorithms of Asymmetric key cryptography; some of the algorithms are RSA, Diffie Hellman, Elgamel etc. [20] [21].

- **The RSA Algorithm :**RSA performs the encryption decryption operations in three parts :

1. Key Generation Process

Select 2 different prime no p1 and p2
Find the value of n where n=p1*p2
Here n is modulus value for both private and public keys.
Find the Euler's Totient Function value
$\phi(n)=(p1-1)(p2-1)$.
Now select the value e which is a public key component and it must follow the following
Condition:
$1<e<\phi(n)$, also e and $\phi(n)$ must be coprime.
Now we have to calculate the private key (d) component, for which the following condition must match
$de \equiv 1 \pmod{\phi(n)}$.

2. Encryption Process

Now communicating parties exchange their public keys and if One wants to send the message To other, the message is encrypted using the recipients public key
as
$C=M^e \bmod n$
Where M = original message
C=Encrypted message

3. Decryption Process

Now recipient uses his/her private key to decrypt the message as follows
$M \equiv C^d \pmod{n}$.

- **Diffie-Hellman Key Exchange Algorithm:**

In Diffie-Hellman Key Exchange Algorithm communicating parties exchange their public keys and after several mathematical calculations a shared secret key is calculated. The calculated secret key is the same for both the users and sometimes it is also known as a session key. The key exchange algorithm has certain limitations as compared to RSA, It's not used for exchanging large data and also vulnerable to the Man-in-the-Middle (MITM) attack [22].

IV. COMPARISON OF VARIOUS DATA SECURITY ALGORITHMS

All the encryption techniques used for security

have their advantages and limitations.

To know which algorithm is best suited for user application is a challenging task as there are numerous algorithms available. So the algorithm must be selected as per application and performance. Every algorithm has certain unique features that can act as deciding factors for the developers and programmers. So there is a need for proper analysis of all the algorithms based on their features. Some of the important factors that decide the performance of algorithms are Encryption time, decryption time, Memory requirements, Throughput, No of keys used, computational speed, key length, etc these factors can be defined as follows

Encryption Time: Time taken by an algorithm to convert plain text to cipher text

Decryption Time: Time taken by an algorithm to convert ciphertext to plain text

No of keys used: Total no of key combinations that are needed to perform the desired operations. No of keys used is an important factor that largely affects the security of the algorithm.

Through Put: It is related to the overall performance of the various resources attached to the system like RAM, HDD, Network related devices, etc. In general, it tells about the amount of data transmitted in a certain time limit.

Computational Speed – Total time taken for encryption and decryption process.

Key Length – Key management plays a vital role in deciding the performance of the algorithms. Symmetric algorithms generally used variable length keys and to select the desired length is algorithm dependent, So key length is selected as per the algorithm to maximize the performance of the system.

Encryption Ratio – The ratio measures the amount of data that needs to be encrypted by the algorithm. It must be minimized which helps id reduction of complexity of computation.

All the algorithms can be compared on the basis of above-mentioned factors as well as some other factors. A table 2 is given below which show the comparative analysis of various cryptographic algorithms based on these factors.

Table2 .Comparison of Encryption Algorithm

Algorithms / Parameters	DES	3DES	AES	Blowfish	RSA	Diffie-Hellman
Type of Encryption	Asymmetric	Asymmetric	Asymmetric	Asymmetric	Symmetric	Symmetric
No of Keys used	The single key used for encryption and decryption.	The single key used for encryption and decryption.	The single key used for encryption and decryption.	The single key used for encryption and decryption.	Two Separate keys used for encryption and decryption.	Key exchange mechanism used.
Throughput	Less than AES.	Less than DES.	Less than Blowfish.	Very High	High	Low
Encryption rate	High	Moderate	High	High	High	High
Key Length	56 bits.	112 to 168 bits.	128,192 or 256 bits.	32 bits to 448 bits.	>1024 bits	Key exchange management.
No.. of Rounds	16	48	10,12,14	16	1	56

Possibility of Modification in key length	No, DES does not support any modification	The key size is increased from 56 to 168 bits	128,192 or 256, Its structure was flexible to multiples of 64	Key length in blowfish should be multiples of 32	Key length in RSA algorithm can be 256 ,512,1024,2048, 4096 bits	No modification in key length.
Developed by	IBM	IBM	Vincent Rijmen, Joan Daemen	Bruce Schiener	Ron Rivest, Shamir & Leonard Adleman	Whitfield Diffie, Martin Hellman
Year of Development	1970	1978	1978	1993	1978	2002
Structural information	Feistel structure	Feistel structure	Feistel structure	Feistel structure	Feistel structure	Tree-based
Cloud Compatibility	Yes but rarely used	Yes	Yes	Yes	Yes	Yes
The algorithm used in Cloud	Not used in Cloud (it is prone to many attacks and easy to break)	Not used in Cloud (it is prone to many attacks and easy to break)	Google Drive, OneDrive, Dropbox	Mozy Backup, Foopchat, GigaTribe	Amazon web Services, RSAWeb	CurveCP
Application areas	Smart Card	Microsoft OneNote, Outlook 2007	Password Manager	IDS Server, SQL Server 2000	Online Credit Card Security System, RSA Signature Verification	In many Protocols like SSL,SSH,IPSec

V. CONCLUSION

As we know cloud computing is growing day-by-day and changing the way of computing and most of the growing organizations opting for cloud-based services as cloud-based services provide cost-effective solutions to these. For all the services, including cloud storage security is the major concern. To overcome the issue of security in cloud-based storage, cryptographic algorithms can be used. In this paper, various algorithms have been discussed and compared. Use of these algorithms and their implementation can be utilized in order to provide security to the user's data. So on the basis of a requirement, these algorithms provides the security in cloud storage systems. As further enhancement, these algorithms can be combined with one another as hybrid approach to provide enhanced security to the user data.

REFERENCES

1. NIST, Cloud Computing Program–29 July 2016: Cloud Computing.Availableonline:https://www.nist.gov/programs-projects/cloud-computing
2. Yadav A.K., Garg M.L., Ritika (2019) Docker Containers Versus Virtual Machine-Based Virtualization. In: Abraham A., Dutta P., Mandal J., Bhattacharya A., Dutta S. (eds) Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing, vol 814. Springer, Singapore
3. L. Kacha and Abdelhafi Zitouni, "An Overview on Data Security in Cloud Computing," Cybern.Approaches Intell. Syst., vol. 661, pp. 250–261, 2017.
4. J. R. N. Sighom, P. Zhang, and L. You, "Security Enhancement for Data Migration in the Cloud," Secure.Enhanc. Data Migr. Cloud, vol. 9, no. 23, pp. 1–13, 2017.
5. https://bigdata-madesimple.com/5-advantages-and-disadvantages-of-cloud-storage/
6. Foster F. Kuhn, D. R., and Chandramouli, R. "Role-Based Access Control, Artech House," 2010
7. https://www.lifewire.com/what-is-cloud-storage-2438541
8. Kumar Yadav, Anuj and Garg, M.L. and Ritika, Dr., An Efficient Approach for Security in Cloud Computing (January 14, 2019). International Journal of Advanced Studies of Scientific Research,Volume 3, Issue 10, 2018. Available at SSRN: https://ssrn.com/abstract=3315609
9. .https://beginnersbook.com/2013/04/advantages-and-disadvantags of-online-data-storage/
10. . http://www.cloudstoragebest.com/pros-ons-cloud-storage-service
11. https://www.lifewire.com/what-is-cloud-storage-2438541
12. https://cloudstorageadvice.com/what-is- cloud-storage/
13. http://www.globalhn.com/blog/advantages-disadvantages-using-cloud-storage-back-data/
14. .https://www.channelfutures.com/industry-perspectives/5-benefits-and--drawbacks-using-cloud-storage-your-baas-offering
15. Kumar Yadav, Anuj & L Garg, M & Mehra, Ritika. (2016). Cloud Data Security using Auditing Scheme. International Journal of Computer Applications. 156. 975-8887.
16. Symmetric Algorithm Survey: A ComparativeAnalysis.International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

17. Comparative Analysis Of Cryptographic Algorithms. Singh et al., International Journal of Advanced Engineering Technology E-ISSN 0976-3945
18. A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306. http://dx.doi.org/10.14257/ijsia.2015.9.4.27.
19. https://www.schneier.com/academic/blowfish/
20. http://www.di-mgt.com.au/rsa_alg.html
21. NaQi, Wei Wei, Jing Zhang, Wei Wang, Jinwei Zhao, Junhuai Li, Peiyi Shen, Xiaoyan Yin, Xiangrong Xiao and Jie Hu, 2013. Analysis and Research of the RSA Algorithm. Information Technology Journal, 12: 1818-1824
22. 22. Akhil Behl "Emerging Security Challenges in Cloud Computing", IEEE 2011

AUTHORS PROFILE

Anuj Kumar Yadav is working as Assistant Professor in the department of Computer Science in Engineering. He is currently pursuing Ph.D. degree in Computer Science & Engg from DIT University,Completed his M.Tech. degree in Computer Science from BIT Mesra, Ranchi and B.Tech from UP Technical University Lucknow. He specializes in core areas of computer science and holds experience of more than 10 years. His area of Interest are Information Security, Distributed Computing Applications and Cryptography.

Madan Garg received the B.E. (Hons) degree in Electrical Engineering in 1974 from Thapar Institute of Engineering & Technology, Patiala, India and the M.Sc. Engineering degree in Electrical Power Systems in 1979 from Punjab Engineering College, Chandigarh. He received the Ph.D. degree in Computer Science & Engineering in 1992 from Thapar Institute of Engineering & Technology, Patiala, India by carrying out the research work at Indian Institute of Technology, Delhi, India. He was Assistant Professor at Philadelphia University, Amman, Jordan from 1995 to 1998. In 2002, he joined University Tenaga Nasional, Kajang, Malaysia. Presently, he is Professor in the Dept. of Computer Science & Engineering, DIT University, Dehradun. His current research interests include Knowledge representation and applications, Fuzzy Logic and
Artificial Neural Networks.

Dr. Ritika is working as an Associate Professor of Computer Science and Applications (Head, Department of Computer Applications) at DIT University. She received her Ph.D. degree in Computer Science from Gurukul Kangri University, Haridwar in the year 2010, M.Tech. degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun and MCA from Gurukul Kangri University Dehradun. She specializes in core areas of computer science and holds experience of more than 17 years. Her area of Interest are Machine Learning, Data Mining and Data ware housing, Mobile and Adhoc Networks. She has life time membership of ISCA, CSI, IEEE, IETE, ACM, IAENG,