Dogo Rangsang Research Journal
ISSN : 2347-7180
UGC Care Group I Journal
Vol-10 Issue-07 No. 16 July 2020

# DATA SLICING AND HYBRID CRYPTOGRAPHY ON MULTIPLE CLOUD STORAGE SYSTEM

**[1]Gogineni Sai Akhil,[2]G.Kaarthikeyan,[3]D.Aswin and [4]Vidhyasagar B.S**
[1]saiakhil123.sa@gmail.com, [2]karthiganapathi15@gmail.com, [3]aswinrockin@gmail.com and[4]vidhyasagar_bs@hotmail.com
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Chennai – 600026.

---

***Abstract:*** Cloud security is getting more important now than ever, but the security for data stored in cloud is still not guaranteed by the cloud providers. This paper proposes a middleware that securely authenticates user, encrypts user files, uploads that to the storage cloud system and vice versa. The middleware used, slices the file being uploaded into multiple parts and names it with random string, encrypts each segmented part with the proposed hybrid cryptographic algorithm then uploads them into multiple cloud storage system. This mechanism of storing and retrieving guarantees data security in cloud environment. We use APIs and libraries provided by cloud providers for implementing this system.

***Keywords:*** Cloud Computing, Hybrid Cryptography, Data Slicing, Cloud Security.

---

## I. INTRODUCTION

Cloud computing is the on demand availability of the computer system resources, especially data storages and computing power, without direct active management by the users. The term is generally used to describe data centers available to many users over the internet. Large clouds, predominant today, often have functions distributed over multiple locations from central servers. The ability to upscale and downscale resources according to the users need is advantageous. This is achieved through proper on-demand administration, resource pooling and virtualization. The availability of high capacity networks, low cost computers and storage devices as well as the widespread adoption of hardware virtualization, service oriented architecture and autonomic and utility computing has led to the growth in cloud computing.

Cloud Storage is a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers, and the physical environment is typically owned and managed by a hosting company. These cloud storage providers responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or applicable data. Cloud storage services may be accessed through a collocated cloud computing service, a web service application programming interface or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

Cloud computing serves on three models, namely

1. Software as a Service (SaaS)
2. Infrastructure as a Service (IaaS)
3. Platform as a Service (PaaS).

Some of the popular storage cloud systems are:

1) Google Cloud:

Google provides a unified and durable storage to the internet. It allows storage and retrieval of any amount of data. Google Drive is a free cloud storage provider which itself relies on Google Cloud, it provides file storage and synchronization service. It provides easy storage and transfer of user data. All Google applications like Gmail, Photos, Notes, Docs, Sheets, Slides etc use Google Cloud as their backend storage.

2) AWS S3:

Amazon S3 stands for Simple Storage Service. It is an object storage service that offers large scale storage. It comprises a simple interface that can be used to upload and later download any amount of data, 24X7 anywhere around the world via internet. It has its own security system that provides various authentication mechanisms to secure data that is stored in Amazon S3 against unauthorized access but still it does not guarantee data security on whole. The common use scenarios include Backup Storage, Application hosting, Media hosting and Software delivery.

3) Rack Space:

Rack Space offers object storage for files, apps and media online. It delivers service globally at very high speeds via world-wide content delivery network. It can able to store any kind of files without any size limitations. The Rack- space system maintains three copies of each file, that are stored in it, so that the users get quicker file access and more reliable storage service. It is powered by the powerful open source technology, OpenStack.

4) QNAP:

ONAP provides high-quality network attached storage service to its users via internet. It uses QSync, a cross device file synchronization system to sync data between the QNAP NAS and other devices like desktops, laptops, tablets and mobile phones to provide flexible collaboration. User can store and access any kind of media or document anywhere and anytime. It also provides a mobile application to remotely take control of data stored in QNAP NAS and stay synchronized.

Since Cloud Computing rest on internet, the user data stored in cloud storage systems are always prone to security issues like data leakage, data theft, data modification, unauthenticated access to data and various hacker attacks. These are mostly due to the weak identity management, patch management, unsafe API's and internal and government threats. Hence to get an overwhelmed acceptance to cloud storage, we have proposed a middleware system that authenticates user, encrypts user files, uploads user data to the storage cloud and vice versa.

## II. LITERATURE REVIEW

Jasleen Kaur and Dr. Sushil Garg,, proposes hybrid algorithm is a combination of two popular and most widely used cryptographic symmetric and asymmetric algorithms.RSA as Digital Signature and Blowfish Algorithm. RSA as Digital Signature is used for authentication and verification purpose and Blowfish is used for encryption and security purpose. RSA falls under public key cryptography. RSA as Digital Signature aims at providing authentication and non-repudiation of the message. It means that the message that the receiver receives is received from the sender and also the message is not duplicated. Two keys are used for signing the document: public key and private key. The private key, is kept secret with the sender and is not shared globally and hence is used for signing the document. The public key is shared globally and is used for authentication of the sender by receiver.

R. Kiruthika, S. Keerthana and R Jeena [9], detailly explains the current security issues that are faced in the cloud computing environment. The author comes up with the proper stats and key issues regarding data security in cloud. Their solution to the issues is through Advanced Encryption Standard (AES) encryption. The author compares the algorithm with various other encryption algorithms in terms of encryptions per minute, hardness of the encryption and time consumption to justify the use of AES for securing the cloud storage. The idea is simply encrypting the data that is stored in cloud storage with AES encryption. The key for the encryption is maintained by a separate physical key management server to add security and this should be installed in the user's premise. The author claims that encryption keys and data stored in cloud storage in secure and under user's control in this method.

Rajiv Mishra and Meenaxi Kumari put forwards the technique of Data Loss Prevention (DLP) mentioning that no data is dispatched to the cloud in straight forward text. DLP is responsible in safeguarding valuable and intimate data and also responsible for not storing private details viz. credit card details, social security numbers, any record details of patients. Since the flow of data takes place from application to application like financial data traversing from credit scoring to that of mortgage originating application its required by the cloud providers to imbibe by the said security standards via access control, encryption.

Vishwanath S Mahalle and Aniket K Shahade [1], presents a Hybrid Cryptographic algorithm to preserve data security in Cloud Systems. The system proposed in this paper is implemented in eye-OS and the hybrid algorithm is made possible by coupling the AES-128 symmetric encryption algorithm and RSA-1024 asymmetric algorithm [1]. The file that need to be stored in the public cloud is stored into a temporary storage and encrypted using AES-128, then uploaded into the cloud storage system. The key of the AES Encryption is again encrypted using the asymmetric RSA encryption using the public key and can only be decrypted using the private key which is only known to the data owner. It is also observed that this can also be used on large files because of its encryption speed and less consumption of computational resource.

Sidharth Sridhar, Arun Muralidharan, Mohammed Ashik and Vidhyasagar B.S, proposes a middleware which uses techniques that involves data slicing and coupling of symmetric and asymmetric algorithm for secured and optimized results. Each cryptographic algorithm follows both the encryption and decryption process. The uploaded file will be split by the middleware's splitter into multiple parts and each part is assigned with random names. Each part then gets encrypted with one of the AES, CAMELLIA and SERPENT algorithms and will be stored into cloud. The applied symmetric algorithm is logged into a file which contains the map of the encryption and associated keys respectively. This file is encrypted with RSA and stored with the same name as the original file name. To retrieve the original data from the encoded cipher, decryption process is carried out. To decrypt, the user's appropriate private key needs to be entered, on successful private key entry the map file gets decrypted and the system parses the respective keys for each segment from the file, merges the segments, recreates the file.

## III. PROPOSED SYSTEM

The proposed system is a middleware that authenticates the user, takes in data from the user, slices the user data by using a slicer module, assigns the sliced data to strings which are named randomly, and later encrypts the individual strings using any of the three algorithms namely AES,CAMELLIA,SERPENT. After the strings are encrypted, they are stored into different buckets of a cloud. The applied symmetric algorithm is logged into a file which contains the map of the encryption and associated keys respectively. This file is encrypted with RSA and stored with the same name as the original file name. The retrieval process is similar to the data insertion process, where the data regarding the initialization, encryption and storage is saved in a log file. To decrypt, the user must enter the appropriate private key, then the map file

gets decrypted and the system gives the respective keys for each segment from the file, merges the segments, recreates the file and makes it available for the user. The system was proposed to enhance the security of the cloud data since it is being widely used by many in today's world.

## IV. System Architecture

The proposed system is a three-tier architecture with multiple sub layers in it. It involves Data Owner/User, Middleware System and the Cloud Storage System. The mode of communication takes place with HTTPS.

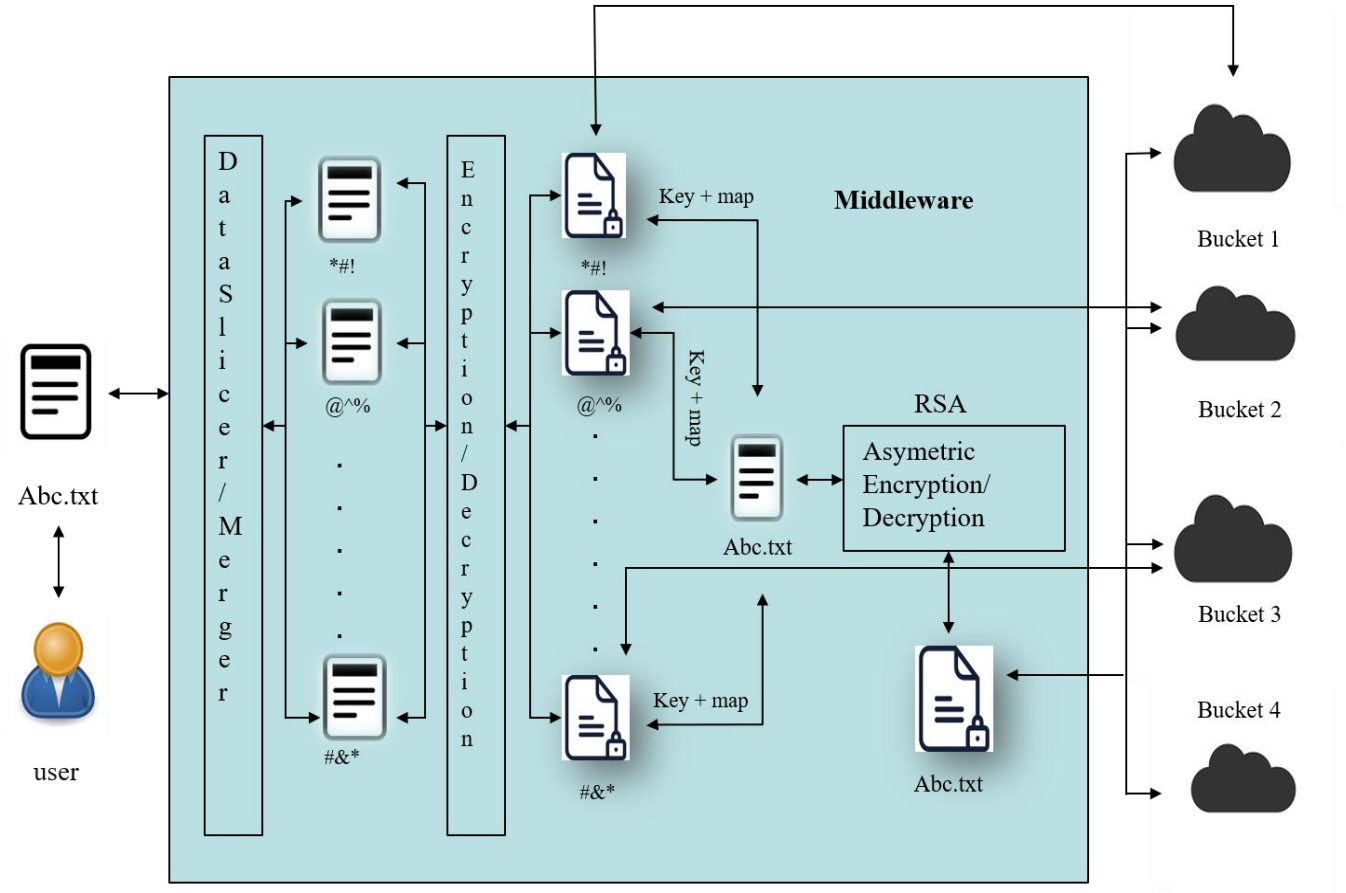



*figure – 1 system architecture*

*A) User:*

The user is an actor who uploads or downloads the file to or from the storage cloud system respectively. He/she can access the system by entering the credentials in the middleware that opens the connection to the storage cloud and able to perform actions in it.

*B) Middleware:*

The middleware is the hub that connects all the components of the architecture. The middleware has three main interfaces in it and are exposed as following components:

*1. Upload/Download*

This is the initial module to get executed on any operation. On uploading the file is sent to the Data Slicing module and are sliced into multiple parts with random names assigned and then sent to the encryption module. On downloading the parts of the files are fetched as per the map file and are sent to the Data Merger module which merges and makes the file available to the user to view or download.

*2. Data Slicing/Data Merging*

On uploading the middleware calls the Data Slicing module which splits the file into multiple parts. The data slicing algorithm divides the total size of the file by n. This involves byte coding. These sliced parts are created by simple I/O system calls.

On downloading, after successful decryption these parts are fetched as per the data in the map file. The Data Merger modules simply appends the start byte to the end byte of the pervious part. Thus, the whole file is recreated same as the original file and are made available to view or download.

*3. Encryption/Decryption*

On Encryption each part of the file is encrypted with random selection of AES/CAMELLIA/SERPENT and are directly uploaded into different buckets of a cloud storage system. The algorithm used to encrypt each part and their respective keys are logged by the middleware system and are stored in a separate file which has the same name as the original file name. This file is encrypted using RSA and stored in multiple buckets of a cloud storage.

On Decryption, the middleware system asks for the user's private key to decrypt the map file, which contains the map and key for the parts of the original file. These are used to decrypt the sliced parts of the file.

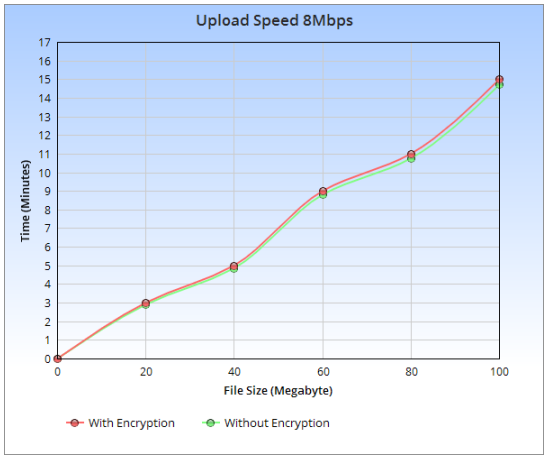
*C) Cloud Storage:*

Cloud storage is the place where the data technically gets stored in cloud. These are the part of cloud computing data centres located in different locations in a protected environment. Data that is processed, transmitted and kept in cloud are logically stored in some storage pools in cloud, and are called cloud storages.

## V. PERFORMANCE ANALYSIS

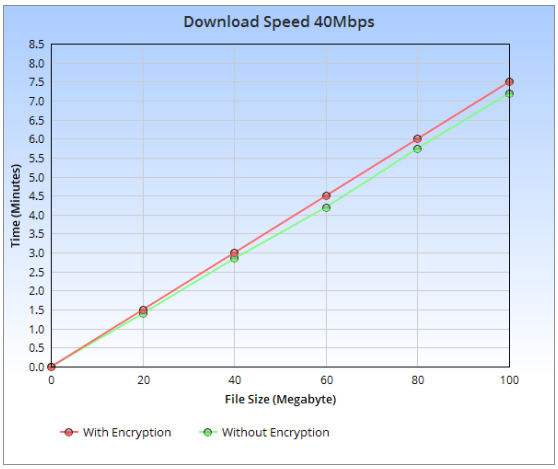
The performance of the system is evaluated based on the time taken by the middleware to upload and download the file to and from the cloud storage system respectively.




*graph 1 – upload time with variable file sizes*

From graph 1, the total execution time taken by the middleware is fairly linear. Minor variations are present only because of fluctuation in upload speed. if the upload speed is stable then the graph would be perfectly linear. Also, the time taken by the encryption is algorithm has a minor impact on the overall execution time of the intermediary(system). For example, to encrypt a 100MB file, the encryption Algorithms take only 2.5s in total. The total time taken to upload includes splitting files into multiple parts, encrypting multiple parts, uploading multiple parts and master file to cloud. Total time for execution mainly relies on the upload speed of the ISP.




*graph 2 - download time with variable file sizes*

Since the download speed is stable, we were able to obtain a linear graph. The time taken for decryption is less than the time taken for encryption because of the preexisting keys and initial vectors (No need to generate random keys and initial vectors again). There is not much variation in time for files uploaded with and without encryption. For downloading the file with decryption, it takes around 7.5s and for downloading the file without any decryption it takes around 7.2s. This time also includes the time to decrypt and merge to recreate the original file. The variation may seem noticeable if the file size is very large, but higher security comes at the expense of higher cost.

## VI. Conclusion and Successive Works

In this paper, we have proposed a new kind of cloud storage security method, where DATA SLICING and the use of HYBRID CRYPTOGRAPHY takes place. The data that is being sent, is sliced, encrypted and stored in different buckets of a cloud storage. This helps in data security a lot as there are three algorithms which are being used in this middleware which prevents attackers from accessing the entire user data. The data is also stored in randomly named strings that prevents the attacker from recognizing the pattern. The user has a private key which is only known to him and this ensures the safety of the cloud data. The middleware asks for the user's private key to access the log file which enhances the total security of the cloud storage devices. Future works involve improving the response time of the system and also making it work in a decentralized environment.

## REFERENCES

[1] Sidharth Sridhar, Arun Muralidharan, Mohammed Ashik and Vidhyasagar B.S Enhanced Cloud Storage Security using Data Slicing and Hybrid Cryptography.

[2] Divya Prathana Timothy and Ajit Kumar Santra, "A Hybrid Cryptography Algorithm for Cloud Computing Security" IEEE Publication, 2017.

[3] Rajiv Mishra, Meenaxi Kumari (2015), "Need of Multi-Layer Security in Cloud Computing for on Demand Network Access", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 4, pp. 398 – 404.

[4] Lovejeet Kamboj, PawanLuthra (2017) "Multi-Layer Data Security in Cloud Computing", International Journal of Computational Engineering Research (IJCER), Vol. 7, pp. 1-7.

[5] Vishwanath S Mahalle and Aniket K Shahade, "Enchancing the Data Security in Cloud by Implementing Hybrid (RSA & AES) Encryption Algorithm" IEEE Publication, 2014.

[6] Jasleen Kaur and Dr. Sushil Garg, "Security in Cloud Computing using Hybrids of Algorithms" International Journal of Engineering Research and General Science Volume 3, Issue 5, September-October 2015.

[7] Kumar, K. Vijay, B. Srinivas Reddy and Dr. N. Chandra Sekhar Reddy, "Preserving Data Privacy, Security Models and Cryptographic Algorithms in Cloud Computing" International Journal of Computer Engineering and Applications, 2015.

[8] Deyan Chen and Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing" IEEE International Conference on Computer Science and Electronics Engineering, 2012.

[9] R. Kiruthuka, S. Keerthana and R. Jeena, "Enchancing Cloud Security using AES Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[10] Dr. Nandita Sengupta, "Designing of Hybrid RSA Encryption Algorithm for Cloud Security", International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 5, May 2015.

[11] Hanumantha Rao, Galli and Dr. P. Padmanabhan, **"**Data Security in Cloud using Hybrid Encryption and Decryption**"** International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013.

[12] S. Munjal1 and S. Garg, "Enhancing Data Security and Storage in Cloud Computing Environment" IJCSIT, Volume 6, 2015.

[13] Shirole Bajirao and Dr. Sanjay Thakur, "Data Confidentiality in Cloud Computing with Blowfish Algorithm" International Journal of Emerging Trends in Science and Technology, IJETST, Volume 1, Issue 1, March 2014.