International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

An Efficient Scheme to Enhance Security of Cloud Storage by Division of Data

Rudragoud Patil, R. H. Goudar

Abstract*: Cloud has become a new paradigm shift in distributed computing. Cloud computing plays an important role in ease of communication, pricing and serving clients in an efficient manner. The adoption of cloud computing is growing rapidly in many organization. Any user can store his data on remote cloud and can be accessed from anywhere, anytime without any hindrance. The most important concerns about cloud storage are security and privacy due to the user sensitive information is stored on cloud. Our proposed scheme reduces both concerns by doing data division, here the user data is encrypted by using Advanced Encryption Standard(AES) algorithm and encrypted file is divided into equal size multiple chunks and stored on multiple cloud servers. The server will take responsibility of placing the chunks into different cloud servers. In our work, we will discuss both schemes like split and encrypt and encrypt and spilt methods and present cryptographic data division after encrypt proves to be better scheme for secure information and it also prevents unauthorized users to access the data. The implementation and results of our proposed scheme is analyzed to address the concerns of cloud computing.

***Index Terms*: Cloud Storage, Encryption, Data Division, Security.**

I. INTRODUCTION

Cloud computing provides the cloud services to the users, clients, organizations, public and etc., as on the pay-as-you-go method. The different components of cloud computing environment are given in Fig 1. In cloud computing security and privacy is the major concern with respect to communication security, data security, network security and virtual machine security. Cloud computing is storing the user data as well as accessing the same with ease of using the internet instead of our memory devices of the computer. Instead of storing the data and running programs from secondary memory storage, cloud computing enables us to access the data as well as run the programs over the internet.Encryption techniques, they effectively secures the client data on public environment called cloud computing. Client can use encryption method on plaintext for security purpose while storing data on cloud, and client can use decryption method to get his own data from the cloud storage. When we talk about cloud data security, it is necessary to focus on different challenges like data at rest, data in communication, data lineage, data recovery because all these concerns may arise from external hackers as well as curious internal personnel of cloud service providers.

Cloud computing services models are classified into following types of cloud services.

- Software as a Service: “SaaS” is a service model that is mainly used to deliver the software’s. In this model applications will be hosted by service provider and these hosted applications are accessible to customers through Internet.
- Platform as a Service: “PaaS” is a service model which enables customers to use the platform that is provided by service provider to develop, manage and run the clients applications. In this model concept of delivering operating systems along with the related services through the Internet without installation or downloads.
- Infrastructure as a Service: “IaaS” is a service model which mainly deals with providing the equipment which is required to execute the operations such as storage, hardware and networking and all these can be given to end customers by using virtualization tools.

The cloud deployment models like private cloud, public cloud, hybrid cloud are used to access any of the above mentioned services based on the customer needs in as pay as you go manner.

Fig. 1. Overview of Cloud Computing

In cloud computing, all the different service models (SaaS, PaaS, and IaaS) will work on one common principle, i.e. clients sensitive data is being processed on cloud servers, which raises different concerns among which security and privacy are major ones, when adoption of cloud computing solution.

Manuscript published on 30 April 2019.
* Correspondence Author (s)
Rudragoud Patil, Research Scholar, VTU RRC, Department of CSE, KLS GIT, Visvesvaraya Technological University, Belagavi, India.
Dr. R. H. Goudar, Department of CNE, Visvesvaraya Technological University, Belagavi, India.

The better optimal solution is to use multiple clouds instead of single private/public cloud. In recent times many such approaches which are employing multiple clouds models are proposed. They may differ in algorithm used, encryption methods, and technologies. In our proposed scheme such similar approach is used for cloud storage security: The user data is encrypted using AES encryption algorithms and divided into multiple chunks and stored on different cloud servers.

This paper is organized as follows in Section II. Brief overview of related literature work is presented. The proposed architecture is given in Section III.Section IV represents implementation of proposed scheme. Section V gives results and analysis of the sheme.Finally conclusion is presented in Section VI.

II. RELATED WORK

Seth B et al. [1] proposed a framework which allows the user to upload encrypted files on to cloud servers and dividing the files into multiple chunks of same size using the concept of crypto database splitting.

Sugumar R. et.al [2] proposed a scheme which divides the files into multiple chunks and also replicates over the multi cloud environment by CTNA (Cloud Tree Node Assignment) and also used minimal cryptographic algorithms to provide security for outsourced data.

Felipe Castro-Medina et.al [3] data division and replication are basic concerns in cloud storage. In this paper authors have presented a novel survey on different methods which are used for above mentioned concerns and also presented web application architecture for data division and replication.

Alsirhani A.et.al [4] authors proposed various encryption algorithms and distributed the encrypted user data on different cloud servers to provide confidentiality of data and also proposed modeling techniques like analytical model and prototype which used emulation to determine the delay of the scheme.

Lentini S. et.al [5] security and privacy are major concerns in cloud environment. In this paper authors presented a report on different data fragmentation methods and also given solutions based on random fragmentation to provide data security to user data which there on cloud storage.

Muthi Reddy P et al. [6] discussed about various methods to protect user private data which is distributed at different cloud servers and designed forward security encryption and re-encryption techniques to provide security for user private data.

S. D. Salunkhe.et.al [7] authors addressed major issue of cloud computing like security and retrieval time of cloud data by doing division of data and also proposed T-coloring concept to identify different cloud servers to store encrypted file chunks.

Suleman nadaf et.al [8] proposed the privacy preserving solution by encrypting the user health data before outsourcing it on cloud storage and also provided keyword search scheme to retrieve files from cloud.

S.Manjula et al. [9] proposed a scheme in which the encryption of file is done by using RSA algorithm and encrypted file is divided into multiple chunks and stored on cloud server. Here concept of cloud manager which runs on server is responsible for storing these chunks into server, but disadvantage of this scheme is cloud manager cannot process the data which raises another concern about confidentiality of user data.

Y. Zhang et al. [10] discussed about match then decrypt method, where the special components which are computed on cipher text files are matched with secret attributes which are in the cipher text to retrieve the files.

Kiraz, M.S et al. [11] discussed about various modern cryptographic methods can be implemented to ensure the high level security and privacy of user personal data which is stored on cloud storage.

Chand K. et.al [12] authors focused about security and performance issues which are addressed by user and cloud service provider. They used a simulation to explore the security and performance parameters to have proper life cycle to deliver services.

Balasaraswathi V et al. [13] present the cryptographic data splitting with dynamic approach for securing information. The metadata information is stored in private cloud. This approach prevents the unauthorized data retrieval by hackers and intruders. The results and implementation for the new proposed model is analyzed, in relation to addressing the security factors in cloud computing.

Ari Juels et al. [14] author's research outcome had come up with solutions where migrate the cloud data into another public cloud but preserving the confidentiality, availability and to achieve these they proposed the framework which uses many modern cryptographic algorithms.

Chia-Wei et al. [15] proposed to incorporate numerical definitions of CSP to have choice in both functionality and cost estimations are defined properly and also proposed algorithms which are efficient to find reasonable solutions in less time.

Kan Yang et al. [16] discussed new access control scheme for multy party computing using CPABE for user data on cloud and also addressed the attribute revocation problem by using new techniques.

III. ARCHITECTURE

The architecture of our proposed scheme is having four components which are shown in Fig.2.

1. Server that stores data onto the cloud and retrieves the data from cloud.
2. Clouds
   - Cloud 'A' that is used to store first half of encrypted file.
   - Cloud 'B' that is used to store another half of encrypted file.
3. Client, where user uses the interface to perform the operations such as encrypt, decrypt, split and merge.
4. Meta Data, which stores information such as user credentials.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

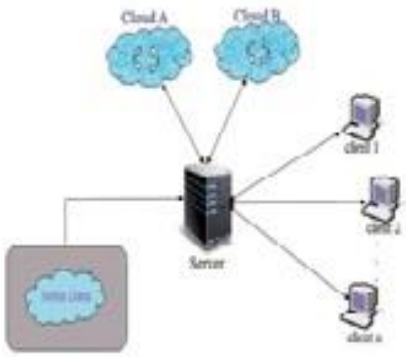

Fig. 2. Architecture of the Proposed System.

IV. IMPLEMENTATION

The proposed scheme is divided into five different modules for implementation purpose. The rest of the section gives an insight into all the modules.

A. Encryption:

Existing encryption algorithms are used effectively used to achieve security of user data stored on cloud. A secret key must be shared between cloud service provider and user to achieve cryptographic operations on file. In our scheme, we have used AES algorithm for encryption and decryption of files.

B. File Split:

File splitting is process of fragmentation of file into equal sized chunks as shown in Fig. 3. Here we select encrypted file which is available in our system and then divide the file into equal chunks based on size and stored them on different cloud servers. The algorithm used for file split is given below.

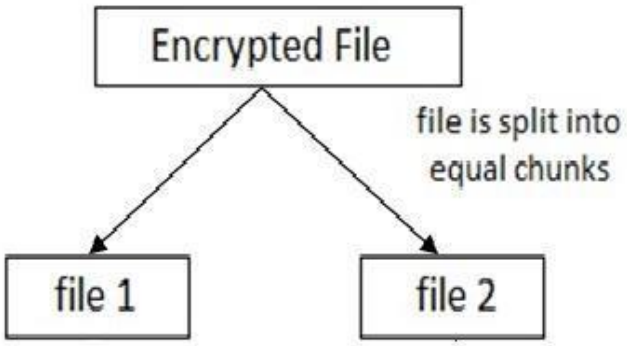

Fig. 3. Splitting of File into Chunks.

Algorithm: File Splitting Algorithm
Input: Cipher text File C(F).
Initializations:
C_k (F) = {$C_1(F^1)$, $C_2(F^{2)}$.....}
F^1=size of(C (F^1))
S_i= $\sum_{i=0}^{n} storageof$ C (F^1) into C_i
Compute:
For each F^1 belonging to C (F)
Select F^1 which has storage S_i
Put F^i in C (F^i)
End

In above stated algorithm, once file is encrypted by using AES algorithm, the cipher text file is divided into multiple chunks of same size then these chunks are stored into different cloud servers by checking availability of servers.

C. Storing file onto cloud:

After encryption and splitting up of the file, different chunks are stored on different cloud servers. Before storing the chunks the current user name is appended with the chunk names and sent to the cloud servers as shown in Fig.4. This is used for the proper authentication during retrieval of files.

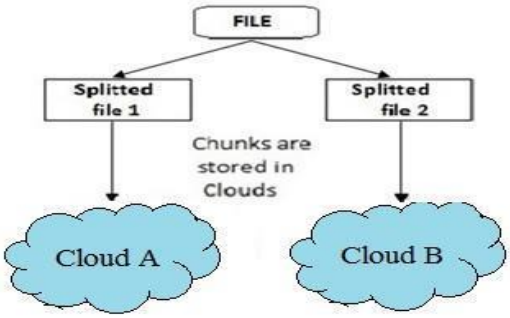

Fig. 4. Storing File into Cloud

D. Retrieving the file:

In retrieving the file from the servers, Client sends the particular file to be fetched from the server. Then server receive the file name and then matches the received file name with the available files stored in server and collects all its related chunks and merge them into a single file, then it sends the content of the file to client as shown in Fig. 4.

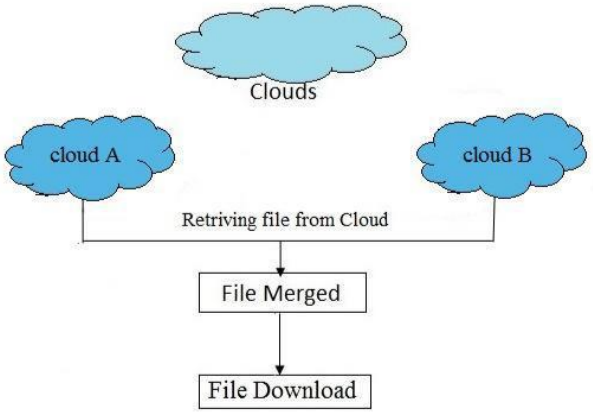

Fig. 5. Retrieving File from Cloud

E. Decryption:

Decryption is reverse process of encryption; here encoded data is converted into plain text form which is readable. All the rounds of encryption algorithm repeat here but in reverse order. The algorithm is implemented using the java code.

Generation of key:

```
KeyGenerator gen = KeyGenerator.getInstance ("AES");
gen.init (128); /* 128-bit AES */
SecretKey secret = gen.generateKey ();
```


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Encryption:

```
Encrypt (Key, InputFile, OutputFile);
doCrypto(Cipher.ENCRYPT_MODE, key, InputFile,
OutputFile);
Cipher.getInstance ("AES"); cipher.init (cipherMode,
secretKey);
```

Decryption:

```
decrypt (Key, InputFile, OutputFile);
doCrypto (Cipher.DECRYPT_MODE, key, InputFile,
OutputFile);
Cipher.getInstance ("AES"); cipher.init (cipherMode,
secretKey);
```

V. RESULT AND ANALYSIS

In our results, we have compared both split-encrypt and encrypt-split methods of dividing the file, before storing on to the cloud servers. Results graphs are drawn by having different file size and for both methods, time in seconds is calculated for different parameters like encrypt, decrypt and split/merge which are shown in Fig.6.(a) and Fig.6.(b) respectively.

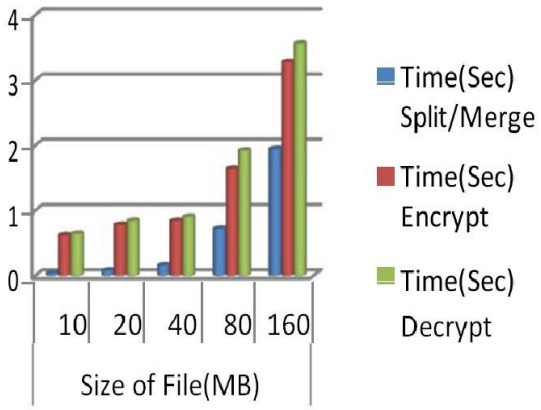

Fig. 6. Graph of Split and Encrypt Method

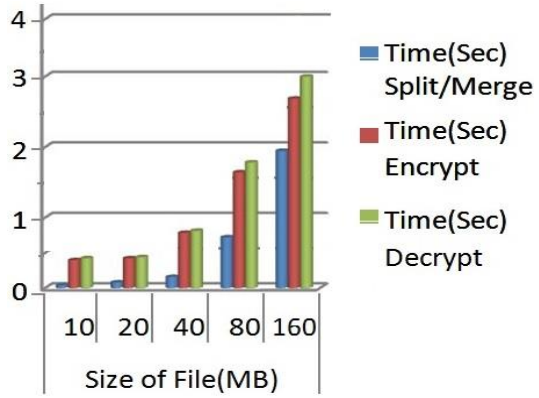

Fig. 7. Graph Encrypt and Split Method

In split and encrypt method, original file is divided first and then these equal sized chunks are encrypted separately and stored onto the multiple clouds. Here the encryption carried on all chunks. But in encrypt and split method, original file is encrypted first and then spilt into equal sized chunks and later stored on multiple cloud servers, where the file is encrypted only once. In the above graphs, we can observe that the encryption and decryption time of encrypt and split method is better than the split and encrypt method.

VI. CONCLUSION

The proposed method provides each end user with ease of using multi cloud storage for better quality of service and to provide security and privacy for sensitive data. By encrypt and split method, data is distributed onto multiple cloud servers. Even if, any intruder gets a part of data from any cloud, it is impossible to decrypt as well as to know the entire data file. With proper validation methods, any end user can store multiple chunks of data onto different cloud servers. The system should have capability to restore and replication of data in case of data loss. Our proposed encryption and split method is better method than split and encrypt method for the contribution to enhance the security of user data which is stored on multiple cloud servers.

REFERENCES

1. Seth B., Dalal S., Kumar R. (2019) Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage. In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence, vol 823. Springer, Cham.
2. Sugumar R., Rajesh A., Manivannan R. (2019) Performance Analysis of Fragmentation and Replicating Data over Multi-clouds with Security. In: Smys S., Bestak R., Chen JZ., Kotuliak I. (eds) International Conference on Computer Networks and Communication Technologies. Lecture Notes on Data Engineering and Communications Technologies, vol 15. Springer, Singapore. pp.1031-1040.
3. Felipe Castro-Medina et.al (2019), "Application of data fragmentation and replication methods in the cloud: a review" International Conference on Electronics, Communications and Computers (CONIELECOMP), pp. 47-54, 2019.
4. Alsirhani A., Bodorik P., Sampalli S. (2018) Data Fragmentation Scheme: Improving Database Security in Cloud Computing. In: Alja'am J., El Saddik A., Sadka A. (eds) Recent Trends in Computer Applications. Springer, Cham.pp.115-138.
5. Lentini S., Grosso E., Masala G.L. (2018) A Comparison of Data Fragmentation Techniques in Cloud Servers. In: Barolli L., Xhafa F., Javaid N., Spaho E., Kolici V. (eds) Advances in Internet, Data & Web Technologies. EIDWT 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 17. Springer, Cham.pp.560-571.
6. Muthi Reddy P, Manjula S. H.,Venugopal K. R.(2017), "Secure Data Sharing in Cloud Computing: A Comprehensive Review", International Journal of Computers.
7. S. D. Salunkhe, D. Patil (2016), "Division and replication for data with public auditing scheme for cloud storage", International Conference on Computing Communication Control and automation (ICCUBEA), pp. 1-5, 2016.
8. Sulemaman nadaf et.al (2016), "Cloud Based Privacy Preserving Health Data Storage and Retrieval System", International Conference on Inventive Computation Technologies.
9. S.Manjual and Dr.M.Indra Devi and R.Swathi(2016), "Division of data in cloud environment for secure data storage", IEEE.
10. Y. Zhang et.al (2016), "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing", Information Sciences 2016.
11. Kiraz, M.S. Journal of Ambient Intelligence and Humanized Computing. (2016) 7: 731. https://doi.org/10.1007/s12652-016-0385-0.
12. Chand K., Ramachandran M., Kor AL. (2015) Simulation of Cloud Data Security Processes and Performance. In: Jahankhani H., Carlile A., Akhgar B., Taal A., Hessami A., Hosseinian-Far A. (eds) Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. ICGS3 2015. Communications in Computer and Information Science, vol 534. Springer, Cham.

13. Balasaraswathi V and Manikandan.S(2014), "Enhanced Security Multi-Cloud Storage using Cryptographic Data Splitting with Dynamic Approach", IEEE.
14. Ari Juels and Alina Oprea(2013), “New Approaches to Security and Availability for Cloud Data”.
15. Chia-Wei Chang, Pangfeng Liu, Jan-Jan Wu (2012), "Probability-Based Cloud Storage Providers Selection Algorithms with Maximum Availability" 41st International Conference on Parallel Processing, pp.199-208.
16. Kan Yang, XiaohuaJia(2011), “Attributed-based Access Control for Multi- Authority Systems in Cloud Storage” in Proceeding of 2012,32nd IEEE International Conference on Distributed Computing Systems ,IEEE.

Authors Profile

Rudragoud Patil, currently working as an Assistant Professor, Dept of CSE, KLS Gogte Institute of Technology, Belagavi. Research Scholar at VTU-RRC, Belagavi. He has 10 years of Teaching Experience. He has published papers in International Journals and Conferences. Her subjects of interest are Cloud Computing, Distributed Computing Network Security and Operating Systems.

Dr.R H Goudar, currently working as an Associate Professor, Dept. of CNE, Visvesvaraya Technological University, Belagavi. He has 14 years of Teaching Experience at Professional Institutes across India. He worked as a faculty at International Institute of Information Technology, Pune for 4 years and at Indian National Satellite Master Control Facility, Hassan, India. He published over 130 papers in International Journals, Book Chapters and Conferences of High Repute. His Subjects of Interest include Semantic Web, Network Security and Wireless Sensor Networks.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)