iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33724

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Chaos Splitting and Merging Security over Distributed Storage in Cloud Computing

Dr. R. Gopi[1], Ms. V. Atchaya[2]
[1]*Associate Professor, Department of MCA, Dhnalakshmi Srinivasan EngineeringCollege, Perambalur, Tamil Nadu.*
[2]*Master of computer Applications, Dhanalakshmi Srinivasan EngineeringCollege, Perambalur, Tamil Nadu.*

Abstract: Cloud Computing facilitates business by storing an enormous amount of data in the cloud transmitted over the Internet with seamless access to the data and no hardware compatibility limitations. However, data during transmission is vulnerable to man in middle, known plain text, chosen cipher text, related key and pollution attack. Therefore, uploading data on a single cloud may increase the risk of damage to the confidential data. Existing literature study uncovered multiple cryptography techniques such as SA-EDS, Reliable Framework for Data Administration (RFDA), Encryption and Splitting Technique (EST) to secure data storage over multi-cloud. However, existing methods are vulnerable to numerous attacks. In proposed system chaos merging technique is used to confuse attackers and protects data from various attackers.
Keywords: Cloud storage, Encryption, Data Transmission, Chaos Splitting and Merging.

I. INTRODUCTION

Be that as it may, cryptography is one of the principal methods used to encipher the data utilizing either symmetric key or asymmetric key. The asymmetric key is considered exceptionally secure as encryption and decryption use different keys. The key generation process of asymmetric key consumes a hug amount of energy and space. Existing proposals have both positives and negatives, for example, Advanced Encryption Standard (AES) is a high-security method used for encryption. Also, Shamir Secret Sharing Scheme is used for encryption. In sensitive data is encrypted by taking XOR with a random number, split and distributed over two clouds. In the author uses a hybrid method such as Advanced Encryptio Standard (AES), Rivest Shamir Adleman (RSA), Blow_sh to secure data. Fully Homomorphic Encryption (FHE) is utilized to encrypt data and then encrypted data is distributed over multi-cloud. In to secure data, AES is used in combination with MD5, however, there is a possibility of a cache-based timing attack on AES. There are chances of Biclique attacks on AES, as proved. Another approach to securely store/transmit data is to part information into equal parts and store it on multi-cloud. To access total information, split parts are blended. Parting information on multi-cloud improves security in such a way that even if an aggressor gains admittance to a part of the data may still be unable to access the full information. This article proposes a symmetric key based cryptographic method named Prescient Security over Distributed Storage (PSDS) to secure client's information over the cloud.

A. Proposed Algorithm

In proposed algorithm chaos splitting and merging technique is used to confuse attackers and protects data from various attackers. A range of file splitting will be done. These splitting will be merged with other file split ups. The number of files and split up will be varied with different users according to the usage.

B. Focal Point

1) Data transmission will be safe from attacks.
2) Even though the data is attacked original data cannot be retrieved from the merged one.
3) The merged data leads the attackers to wrong data.

II. ENVIRONMENT DETAILS

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

1) Software Specification

a) Front end = java 8 and above
b) Back end = MySql 5 and above
c) Tool = netbeans 8.0 and above

2) Hardware Specification

a) Processor =Intel i3 and above
b) Ram =4 GB and above
c) Hard disk =250 GB and above

A. System Architecture

1) Single and Mulite Cloud Server Construction

a) Users will be registered in cloud server.
b) Single and multi cloud access is set.
c) Storage size is allocated.
d) Cost maintenance for different cloud will be done.

2) Constructing Range For Splitting And Merging

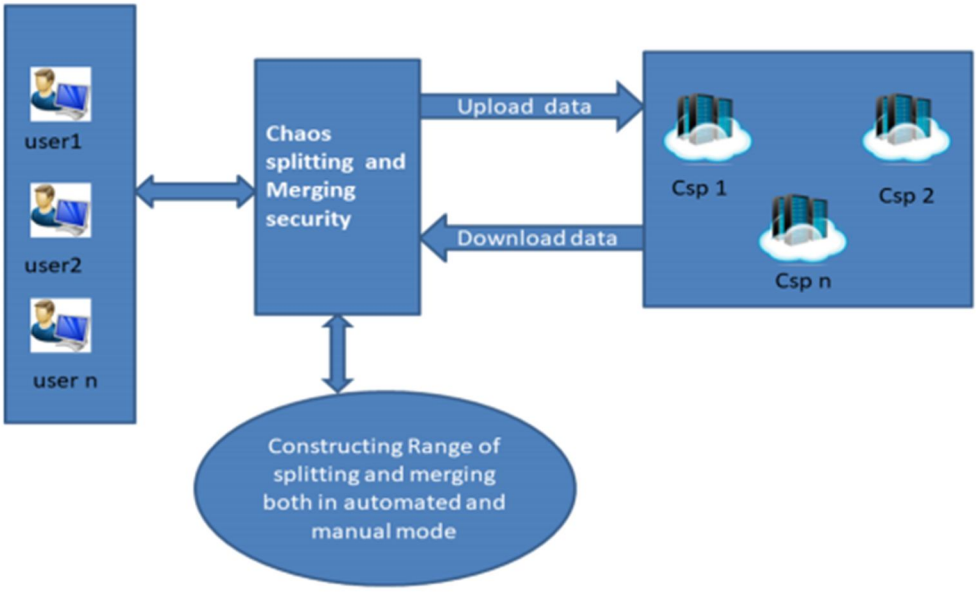
a) Range will be set for splitting up of files.
b) The range depends upon the size of the file.
c) Number of files to be selected for Merging will also comes under different range.

3) Automatic And Manual Mode For Securing

a) Automatic and manual mode will be provided for users.
b) In automatic mode the default range will be selected for both split ups and merging.
c) Low ,medium and high sensitivity will be the range available in manual mode.

4) Retrieving Orginal Data

a) Retrieving original data will be done by extracting specific files with the help of metadata.
b) These metadata will be secured in client system.
c) After downloading the files will be merged with its own parts.



©IJRASET: All Rights are Reserved

B. Software Overview

Java is a platform Independent. Java is a high level programming language Introduced by Sun Microsystems in June 1995 Java is becoming a standard for Internet Applications. It provides for interactive processing and for the use of graphics and animation on the Internet. Since the Internet consists of different types of computers and operating systems, a common language was needed to enable computers to run programs that run on multiple platforms. Java is an object oriented language built upon C and C++.It derives its syntax from C and its object-oriented features are influenced by C++. Java can be used to create applications and applets. An application is a program that runs on the user's computer, under its operating system. An applet is a small window based program that runs on HTML page using Java enabled browser like Internet Explorer, Netscape Navigator, Hot Java or an applet view

1) Features of JAVA

Simple

a) Java Language constructs are easy to learn and use. It takes care of memory management. Though

b) Java was developed from C++, the complexities associated with C++ have been eliminated in Java.

2) *Object-Oriented:* Java is designed around the object-oriented model. In Java the focus is on the 'data' and the 'methods' that operate on the data in an application and not just on the procedures. The data and methods together describe the state and the behaviour of an object in Java.

3) *Robust:* Java is a robust language since it has strict compile time and run time checking of code. This minimizes programming errors. Error handling and recovery is taken care of in Java by the 'exception- handling' feature.

4) *Secure:* Java is language that focuses on the network. Java security features ensure that its programs that run are safe. Programmers cannot manipulate memory in Java. This is a good defense mechanism against malicious code that may flow in from the network. Java programs running on the Web cannot open, read, write or delete files on the user's system or run other programs on it.

5) *Distributed:* Java can be used to develop applications that are portable across multiple platforms, operating systems and graphical user interfaces. Java is designed to support network applications. Thus Java is widely used tool in an environment like the Internet where there are different platforms.

6) *Multithreaded:* Java programs can do many tasks simultaneously by a process called 'multithreading'. Java provides the master solution for synchronizing multiple processes. Therefore, interactive applications on the Net can run smoothly. This is made possible by the built-in support for threads.

a) Running Java File with single command

b) New utility methods in String class

c) Local-Variable Syntax for Lambda Parameters

d) Nested Based Access Control

e) HTTP Client

f) Reading/Writing Strings to and from the Files

g) Flight Recorder

C. Technology Infrastructure

1) *Core Java:* Java can be used to create two types of programs: application and applet. An application is a program that runs on your computer, under the operating system of that computer. That is, an application created by java is more or less like one created using C or C++. When used to create application, java is not much different from any other computer language. Rather, it is java's ability to create applets that makes it important. An applet is an application designed to be transmitted over the internet and executed by a java-compatible Web Browser. An applet is actually a tiny java program, dynamically downloaded across the network, just like an image, sound file, or video clip. The important difference is that an applet is an intelligent program, not just an animation or media file. In other words, an applet is a program that can react to user input and dynamically change-not just run the same animation or sound over and over.

©IJRASET: All Rights are Reserved

D. System Maintenance

System maintenance is an ongoing activity, which covers a wide variety of activities, including removing program and design errors, updating documentation and test data and updating user support. For the purpose of convenience, maintenance may be categorized into three classes, namely:

1) Corrective Maintenance: This type of maintenance implies removing errors in a program, which might have crept in the system due to faulty design or wrong assumptions. Thus, in corrective maintenance, processing or performance failures are repaired

2) Adaptive Maintenance: In adaptive maintenance, program functions are changed to enable the information system to satisfy the information needs of the user. This type of maintenance may become necessary because of organizational changes which may include:

a) Change in the organizational procedures,
b) Change in organizational objectives, goals, policies, etc.
c) Change in forms,
d) Change in information needs of managers.
e) Change in system controls and security needs, etc.

E. Perfective Maintenance

Perfective maintenance means adding new programs or modifying the existing programs to enhance the performance of the information system. This type of maintenance undertaken to respond to user's additional needs which may be due to the changes within or outside of the organization. Outside changes are primarily environmental changes, which may in the absence of system maintenance, render the information system ineffective and inefficient.

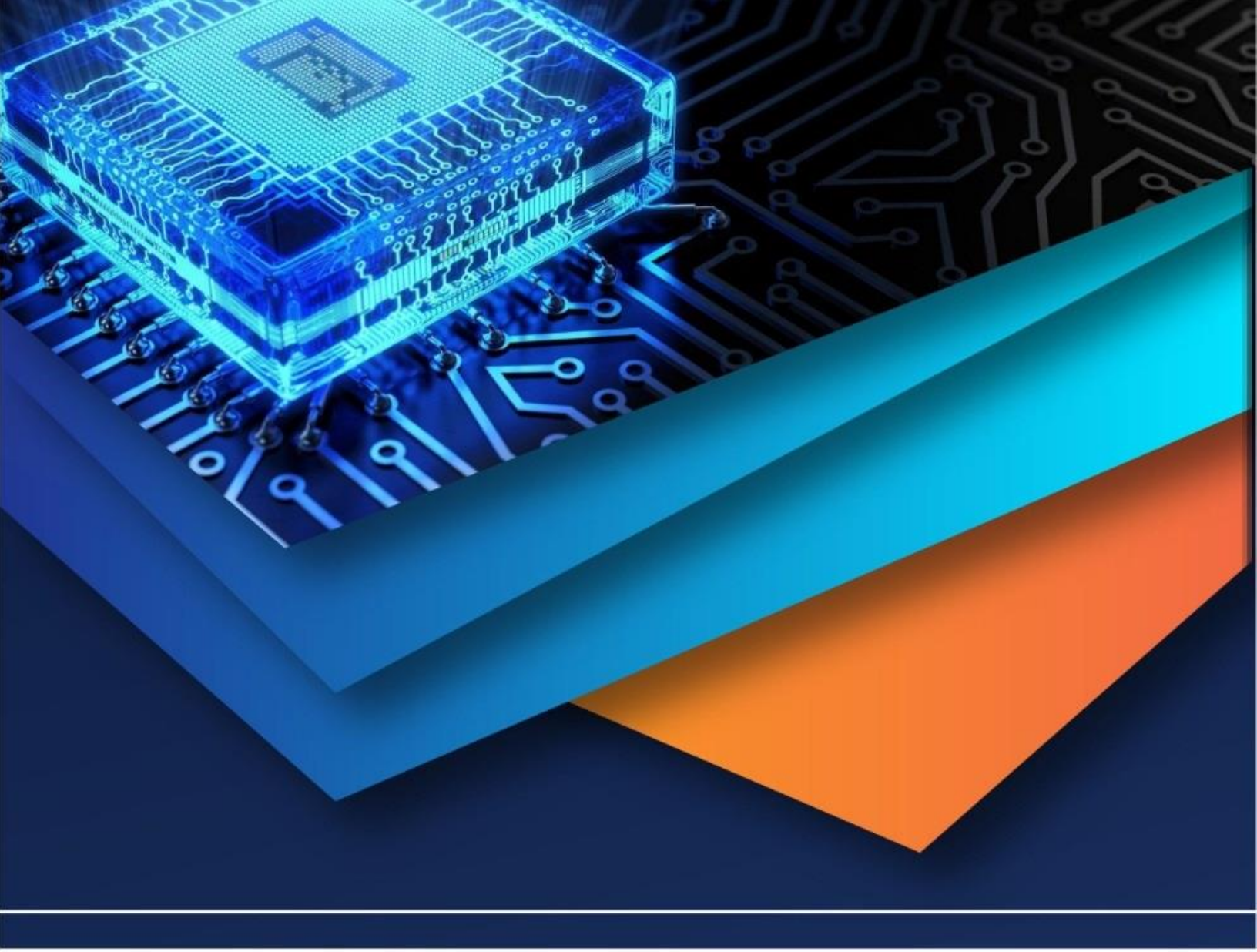
III. CONCLUSION

Cloud computing becomes common among people, as people can easily save their huge amount of data in order to save memory consumption. The major issue in storing data on clouds is data security. There is a need to transfer data into cipher text. Multiple approaches are used to secure data over the cloud. Computational time is focused on data security approaches. A complex algorithm is not suitable for data security due to their increasing computational time. The less complex algorithm has security issues. In this paper, we propose chaos splitting and merging in order to solve the issue. It divides the data in normal and sensitive part. Normal data is encrypted and uploaded over a single cloud while sensitive data is divided into two parts, then encryption steps are applied on these two halves and uploaded on separate clouds. At the time of downloading, these two separate halves are merged and the decryption algorithm is applied in order to obtain plain text. The proposed approach is secure against chosen cipher text, known the plain text, related-key attack, pollution attack, and main-in middle attack.

REFERENCES

[1] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, "Attribute based encryp- tion in cloud computing: A survey, gap analysis, and future directions," J. Netw. Comput. Appl., vol. 108, pp. 37–52, Apr. 2018,
[2] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," Future Gener. Comput. Syst., vol. 56, pp. 684–700, Mar. 2016.
[3] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Proc. Inf. Secur. South Africa, Aug. 2010, pp. 1–7.
[4] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, "Content based double encryption algorithm using symmetric key cryptography," Procedia Comput. Sci., vol. 57, pp. 1228–1234, Jan. 2015.
[5] R. F. Olanrewaju, B. U. I. Khan, A. Baba, R. N. Mir, and S. A. Lone, "RFDA: Reliable framework for data administration based on split-merge policy," in Proc. SAI Comput. Conf. (SAI), Jul. 2016, pp. 545–552.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)