A Framework for Cloud Computing Data Security and Privacy

Reetesh Rai[1], Dr. Ravindra Tiwari[2]

[1]Research Scholar, [2]Guide

[1,2]LNCT University, Bhopal

Abstract - One of the most difficult problems affecting cloud computing systems' reliability is ensuring the security and privacy of data kept on cloud servers. The most popular method for increasing cloud server dependability and safeguarding resources from potential attacks and unpredictable events is the application of cryptography algorithms. In a cloud computing environment, the user's data is stored on a server, and the company's service providers are held responsible for its security. The service provider looks after the security of the clients' data. The issue with the cloud computing system is that service providers treat all data in the same way, which results in their offering a common level of protection to all data for a certain user without taking into account whether or not that security is necessary. In order to address this issue, we suggested the idea of data classification. According to the data's secrecy, we divide the data in our proposed work into groups, and each category is given its own level of protection. This idea allows us to decrease overhead while increasing processing speed. It may also improve the efficiency of the cloud environment. For the security of the data, the suggested approach uses a different encryption algorithm. Data that needed high security are given high security, and data that wanted low security are given low security, using our recommended work. The work being done now is safer and more effective than previous labour.

Keywords: - Cloud Computing, Data Classification, Data Security, File Splitting, Single Encryption, Multiple Encryption.

I. INTRODUCTION

The most promising technology today is cloud computing, which has recently entered the real world. Users are beginning to use cloud computing as they become more aware of its benefits. The technology of the future, known as cloud computing, offers a simple and adaptable method of handling data on the Internet. It offers the user a number of services for using cloud applications and gaining access to them. Users can upload their data to cloud storage and view it from any location using a variety of devices, including laptops, desktop computers, mobile phones, etc. Users own data, which is necessary, important, and useful. Any type of data is possible, including documents, films, photographs, and more. Every time data are discussed, some of their characteristics become apparent. Accuracy, completeness, consistency, and other terms are a few of them.

Cloud data primarily deals with three security challenges. Confidentiality, availability, and integrity Data should be kept private and confidential from others. Users who are not authorised or authenticated cannot access or utilise the data. Data integrity means that the data's content shouldn't be compromised. According to some, maintaining data is necessary to achieve accuracy and consistency. Data should be accessible for users when they need it; this is known as availability. It is necessary to perform adequate recovery and backup management in order to achieve the availability of the data in the correct storage type.

The goal of cloud service providers (CSPs) is to provide customers with the same type of environment that customers receive from ISPs (ISPs). Similar to how both provide administrations and work in a distributed environment, etc. As it powers up the computing and gives the client access to the system in their interest, distributed computing has offered some additional benefits to cloud computing. Some security-related problems are encountered by the Distributed Computing Innovation.

II. ISSUES IN CLOUD ENVIRONMENT

The three deployment models are private cloud, public cloud and hybrid cloud. The security issues of these deployment models are discussed below [6].

A. Security issues in a public cloud

In a public cloud model, the platform and infrastructure are shared among customers. The securities for these services are provided by the cloud service provider. A few of the key security issues in a public cloud include:

1) Since there is no control over the security mechanisms used by the cloud service provider, it is difficult to protect data in all its stages providing the basic requirements of confidentiality, integrity and authenticity.

2) Since most service providers use a multitenant architecture hence the possibility of data leakage between the tenants is very high.

3) If the Cloud service provider uses a Third-Party vendor for providing the services, then there is added overhead of verifying the agreements and contingency plans between them.

4) There is also a possibility of an insider attack at the service provider side. As the cloud architecture grows the number of insiders grow. Proper laws should be enforced to protect data from malicious insiders.

B. Security issues in a private cloud

A private cloud model enables the customer to have local network and storage space. They provide the flexibility to the customer to implement any kind of required services. There are certain securities issues:

1) Due to virtualization, unauthenticated and unauthorized access to system is possible

2) Malware can be used to attack the host operating system.

3) Security policies must be designed to protect attacks from insiders.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud model. Each of the three ways in which cloud services can be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them [6].

III. LITERATURE REVIEW

Numerous projects have been undertaken in the area of cloud computing. Security in the cloud has been the subject of numerous methodologies and works. Several are covered below: -

M. Sasikumar, Rizwana Shaikh, This study is a survey that looked at cloud computing security concerns. The author of this article highlighted some security challenges that clients and providers of cloud computing may encounter. He also focuses on the answers to some of the problems. [1] Mr. Rupesh R. Bobde, Dr. M. M. Raghuwanshi, and Amit Khaparde developed a plan in which the original data are divided into several slices. Before being stored in the cloud, the data in each slice can be encrypted using a variety of cryptographic techniques and an encryption key. The goal of this method is to store data properly, securely, and safely in order to prevent invasions and data attacks, while also lowering the cost and time associated with storing encrypted data in cloud storage. [3] Raad S. Al-Qassas, Fahd Aldosari, Lo'ai Tawalbeh, Nour S. In this essay, the author identifies the issue with cloud computing, which is that all data is not handled equally or with the same level of security. As a solution to the aforementioned issue, he put forth a framework that divides data into three categories—Basic, Confidential, and High Confidential—and offers various security techniques depending on the situation. Basic data would receive very little security, Confidential data would receive moderate security, and High Confidential data would receive high security. [4] Gurpreet Singh and Miss Supriya conducted a thorough analysis of well-known encryption algorithms as RSA, DES, 3DES, and AES. This study conducts an overview of the previous efforts on encryption techniques. In conclusion, real-time encryption can benefit from all of the strategies. Each technique is distinctive in its own right, may be appropriate for various purposes, and has advantages and disadvantages of its own. They discovered that the avalanche effect, speed, duration, and throughput of the AES algorithm are all at their highest levels. [5]

Sanjay Agrawal and Ritu Tripathi conducted a survey of symmetric and asymmetric cryptography techniques. The performance of a few symmetric and asymmetric encryption algorithms, including DES, 3DES, AES, Blowfish, RSA, and Diffie Hellman, is evaluated in this work. With asymmetric encryption, the key length is longer. In RSA, it is difficult to crack the code because of the long key length. When it comes to throughput, throughput grows and power consumption falls. Since blowfish has a high throughput and a low power need, it is considered to have good speed for symmetric key encryption. Finally, the blowfish method is recommended as the superior choice for symmetric key encryption schemes. The RSA algorithm is safer when using asymmetric encryption since it factors large prime numbers to create keys. [6]

IV. PROBLEM STATEMENT

According to the literature analysis, there is a difficulty with every firm adopting the same software for data encryption across the board in the Cloud Computing environment. By using a single piece of software, all data is handled uniformly. This is a disadvantage of utilising a single piece of security software without taking the importance or how sensitive the data is into account. The classification of the data is the solution to the issue now that it has been identified. Sort data into categories, then give security in accordance with those categories.

V. PROPOSED SYSTEM

We have divided or classified the data in our proposed work into three categories: general data, secured data, and highly secured data. In our work, manually categorized data is data that has been classified by the users themselves. Every user is more familiar with their own data than other users, which is why the classification handbook was created. He merely is aware of which of their info genuinely needs greater security or not. Additionally, the user has the ability to decide whatever data he wants to be more or less protected.

General Data: All information that consumers desire to be protected with minimal security is contained inside general data. They receive lower-level security for the data that falls within this category. We are employing the AES 128 Encryption technique for lower-level security.

Secured Data: This is another category that includes data that requires a certain level of protection. Security that is higher than general data but lower than highly secured data is referred to as moderate security. We employ the AES 256-bit encryption technique for Secured Data.

Highly Secured Data: This category offers the highest level of data security. All of the data in this category are protected with the best security measures. In this case, the concept of file splitting is used in our suggested work to provide great security. The entire file is divided into three chunks, each of which is encrypted using TDES, AES-128 and AES-256.

Splitting files: We have incorporated a notion known as file splitting in our proposed work. The method or technology known as "file splitting" separates a certain file into portions. Here, the little components of files are referred to as chunks. The pieces are then stored in various locations, and when that file is needed, all of the chunks are collected from their locations and combined to create the original file. Increased execution time is the key benefit of file splitting. When processing time is a concern, breaking a file into smaller chunks and processing each one separately will be a good alternative. This will speed up processing.

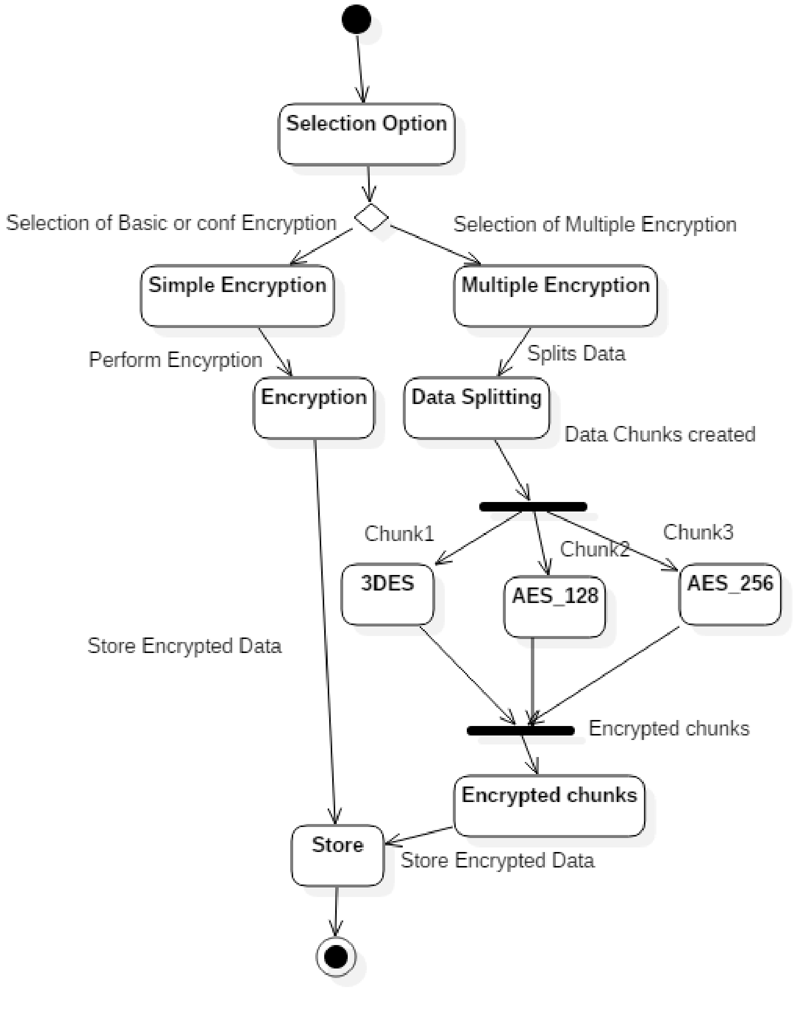
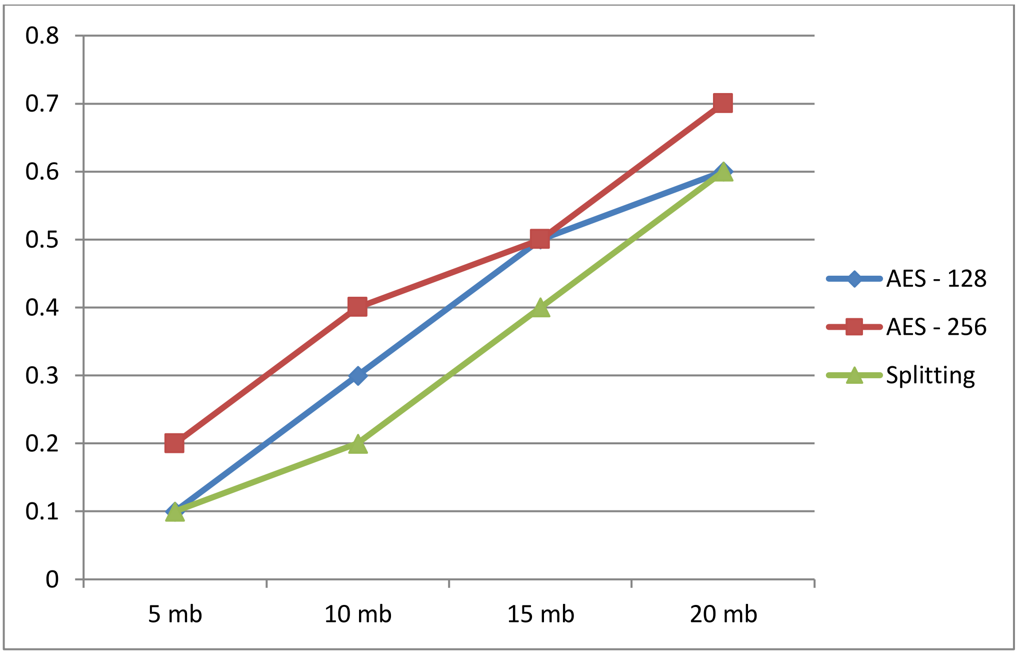


Fig 1: State chart diagram for Overall System

VI. RESULT AND COMPARISON

We designed a web environment that is similar to what a user would find in the cloud for the purpose of implementing our suggested task. The user can select between uploading a file and viewing one that has already been uploaded from an interface that includes both options. The user is taken to the browser page where he must select the file from his local storage when he chooses the "Upload File" option. After selecting the file, the user must additionally select the specific security level for the uploaded data; this will determine the level of encryption protection for the user's data. We determine the time required by the various user-selected options—whether they are general, secure, or very secure—and compare them to arrive at the indicated conclusion. AES128 has been used for ordinary encryption, AES256 for secure encryption, and file splitting for more secure encryption.



The above graph shows the time taken by the different security algorithm to encrypt the different size data 5mb, 10mb, 15mb and 20mb. In this graph we have show the following security algorithms AES-128, AES-256 and our File Splitting Security algorithm and time taken by them to execute the data. With the help of graph it is clear that splitting takes less time and provides more security.

VIII. CONCLUSION

The cloud computing industry is still in its infancy, but it is growing as time goes on. The number of people using the cloud is growing along with it, and this poses a serious threat to the security of the data kept on the cloud server. In our work, we've talked about security algorithms like TDES and AES-128/256 and compared them. Additionally, we have added a brand-new security feature based on file splitting. We may infer that our work is an efficient and effective secrecy-based system by carefully examining all the findings and graphs of the suggested work that it improves the cloud environment's performance and decreases processing time. They receive that level of security in accordance with the information's requirements as well. The framework demonstrates that our suggested work offers superior security to competing solutions.

As a part of the future work in relation to our proposed work, this can be improved with better security algorithms like asymmetric algorithms with better execution times, new techniques and methods used for providing better security to the information, and alternative methods of data classification can also be used which enhance the system. Additionally, soft computing approaches that offer automatic data classification and better methods for maintaining the secrecy and integrity of the information can be used.

REFERENCES

[1] Security Concerns in Cloud Computing: A Survey, Rizwana Shaikh and M. Sasikumar, International Journal of Computer Applications, 2012.

[2] Dr. M. Sasikumar, Rizwana Shaikha In cloud computing, "Data Classification for Achieving Security" pp. 493–498 in Science Direct Procedia Computer Science 45 (2015)

[3] An Approach for Securing Data On Cloud Using Data Slicing And Cryptography, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015, by Mr. Rupesh R. Bobde, Amit Khaparde, and Dr. M. M. Raghuwanshi

[4] A secure cloud computing model based on data classification was developed by Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, and Fahd Aldosari. Science Direct Procedia Computer Science 52 (2015) 1153–1158.

[5] Singh, Gurpreet, and Supriya International Journal of Computer Applications (0975 - 8887) Volume 67- No.19, April 2013, "A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security"

[6] Sanjay Agrawal and Ritu Tripathi Symmetric and asymmetric cryptography techniques: A Comparative Study Volume 1, Issue 6 of the International Journal of Advance Foundation and Research in Computers (IJAFRC). ISSN 2348 – 4853

[7] Frank Simorjay, "Data Classification for Cloud Readiness," Microsoft Trustworthy Computing Doc. 2014.

[8] Science and Information Conference 2015 July 28–30 | London, UK Fara Yahya, Robert J Walters, and Gary B Wills "Protecting Data in Personal Cloud Storage using Security Classifications"

[9] Zurina Mohd Hanapi and Nasrin Khanezaei A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services was presented at the 2014 IEEE Conference on Systems, Process, and Control (ICSPC 2014),

which took place in Kuala Lumpur, Malaysia, from December 12 to December 14.

[10] S. Monikandan and Dr. L. Arockiam, "Efficient Cloud Storage Confidentiality to Ensure Data Security," International Conference on Computer Communication and Informatics (ICCCI-2014).

[11] A Probabilistic Integrity Checking Approach for Dynamic Data in Untrusted Cloud Storage, 978-1-4799-0174-6/13/$31.00 2013 IEEE, Thanh Cuong Nguyen, Wenfeng Shen, Zhou Lei, Weimin Xu, Wencong Yuan, Chenwei Song.

[12] Top Threats to Cloud Computing V1.0, 2010, CSA.