Research Result

A Framework to Achieve Data Security and Privacy in Cloud Computing

Neha Pandey[1], Prof. Saurabh Sharma[2]

[1]*M.Tech. Student, Computer Science Engineering, Global Nature Care Sangathan's Group of Institutions, Jabalpur (M.P.), INDIA*
[2]*Assistant Professor and HOD, Department of CSE, Global Nature Care Sangathan's Group of Institutions, Jabalpur, (M.P.), INDIA*

ABSTRACT

One of the most difficult problems that reduces the rate of reliability in cloud computing environments is making sure data stored in cloud servers is secure and private. The most frequent approach to improving the security of cloud servers and shielding their resources from attacks and unforeseeable events is to employ cryptography techniques. In a Cloud Computing setup, the user's data resides on a server, and the responsibility for the data's safety falls on the shoulders of the service providers. The provider will ensure the safety of the clients' information. The difficulty with the cloud computing system is that the service providers treat all the data in the same way, which means they supply common protection to all the data for the individual customer without assessing whether or not that data actually needs that security. Therefore, we presented the idea of data classification as a means of dealing with this issue. In the work we propose, we divide the data into groups according to how secret each piece of information is, and then we secure each category of data with its own set of safeguards. The use of this idea allows us to cut down on unnecessary work and speed up the processing time. Additionally, it can boost cloud performance. The information is encrypted utilising a variety of algorithms in the proposed approach. With our plan in place, data that needs a high level of security can get it, and data that wants a low level of security can get it. When compared to previous efforts, this one is safer and more effective.

KEYWORDS

Cloud Computing, Data Classification, Data Security, File Splitting, Single Encryption, Multiple Encryption

1. INTRODUCTION

Cloud computing is the most exciting new technology to appear in recent years. The benefits of Cloud Computing become well known to users, who begin adopting it. Cloud computing is a cutting-edge system that simplifies and personalises the management of data in the cloud, or online storage space. Different services for interacting with Cloud applications are made available to the user. The Cloud allows users to store their information in a central location that they can access from any computer, smartphone, tablet, etc. Users' data is something vital, important, and valuable. All sorts of media, including text files, movies, image files, and audio recordings, can all be considered data. Some data properties always come up when talking about data. Accuracy, Fullness, Consistency, Etc.

There are three main concerns when it comes to the safety of cloud-based data. No one but authorised parties will have access to your data, and your data will always be secure and readily available. Data This means that information should not be shared with unauthorised parties. No one who isn't allowed or authenticated can see or use the information. By ensuring data integrity, we ensure that the information contained inside the data is not altered in any way. It has been argued that data must be kept for reliability and precision. Availability refers to the state of having data readily accessible when a user requests it. Achieving data availability requires the application of recovery and backup management strategies appropriate for the storage medium.

CSPs, or cloud service providers, are aiming to provide their customers with an identical setting to that provided by ISPs (ISPs). They're similar in that they both provide administrations and use the Distributed Environment. When combined with Cloud Computing, distributed computing boosts processing speed and gives users flexible system access. There are a few safety concerns with the Distributed Computing Revolution.

2. 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].

3. LITERATURE REVIEW

There is various work done in the field of Cloud Computing. Many methods and work have been proposed related to security in Cloud. Some are discussed below: -

Rizwana Shaikh, M. Sasikumar, this paper is the survey paper which surveyed the security issues in cloud computing. The author is this proposed the different security concerns, what are the security issues the Client and the Providers facing in the Cloud Computing. For some of the issues he also focuses on the solutions.[1]

Mr. Rupesh R Bobde, Amit Khaparde and Dr.M. M. Raghuwanshi proposed a scheme in which the original data get sliced into different slices. The data in each slice can be encrypted by using different cryptographic algorithms and encryption key before storing them in the Cloud. The objective of this technique is to store data in a proper secure and safe manner in order to avoid intrusions and data attacks meanwhile it will reduce the cost and time to store the encrypted data in the Cloud Storage.[3]

Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd Aldosari, In this paper the author find out the problem in Cloud Computing and the problem is treating all the data in same manner and providing same level of security. As a saluting for the above problem, he proposed a framework which classify the data into three categories say Basic, Confidential and High Confidential and providing the different security techniques according the requirement like Basic get very less security, Confidential get moderate security and High Confidential get High security.[4]

Gurpreet Singh and Miss Supriya performed a detailed study of the popular Encryption Algorithms such as RSA, DES, 3DES and AES. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. They found that AES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect. [5]

Ritu Tripathi, Sanjay Agrawal performed a survey on symmetric and asymmetric cryptographic methods. This paper presents a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen The key length is higher at the Asymmetric encryption technique. The high key length makes to break the code complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques the blowfish algorithm is specified as the better solution. In the Asymmetric encryption technique, the RSA algorithm is more secure since it uses the factoring of high prime number for key generation. [6]

4. PROBLEM STATEMENT

According to the literature review we have found out that in the entire Cloud Computing environment, there is a problem that all the organizations, using the single software for the encryption of the data. Single Software means they all treat whole data in a same manner. This is the drawback of using single software for the security without considering the sensitiveness or criticalness of the data. Now after the detection of the problem the solution for this is the classification of the data. Classify data into categories and according to that provide Security.

5. PROPOSED SYSTEM

Our suggested work classifies information into three broad buckets: public, protected, and secret. We have found that having consumers manually categorise data yields the best results. The classification guide was created because each user has unique insights into their data. He is the only one who knows for sure which of their records calls for further protection. The user can also decide how much protection to provide for different pieces of information.

All user data that has to be protected with a minimal level of security is kept in general data. For this type of information, they just bother with the most basic security measures. We are encrypting with AES-128, which is a weaker method but still effective for lower-level security purposes.

Information requiring a moderate level of security is included in the Secured Data category. Data with a moderate level of protection is more secure than basic

information but less so than highly protected data. Here at Secured Data, we encrypt everything using AES 256-bit encryption.

Information in this category has the greatest possible level of protection. All of the files in this folder have been given the highest level of protection possible. We propose using the idea of "File Splitting," in which a single file is broken up into three smaller parts and encrypted independently using TDES, AES-128, and AES-256, for maximum security.

Separating Data: We've used a technique called "File Splitting" in our proposed work. File splitting is a method of separating large files into more manageable pieces. The atomic units of files are referred to as "chunks" here. When a file is too large to transfer in its entirety, it is broken up into smaller pieces called "chunks," which are then stored separately. In order to speed up the program's execution, file splitting is crucial. When time to execution is critical, it may be beneficial to break up large files into smaller chunks and process those separately.

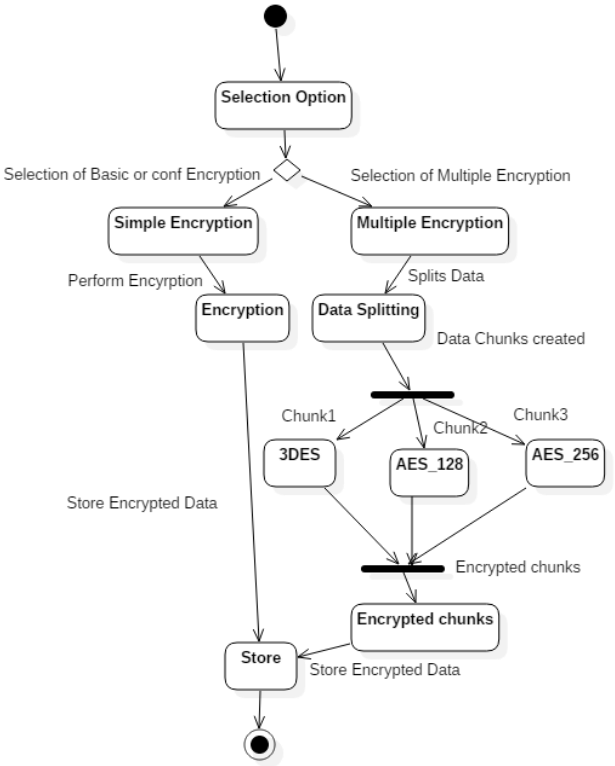
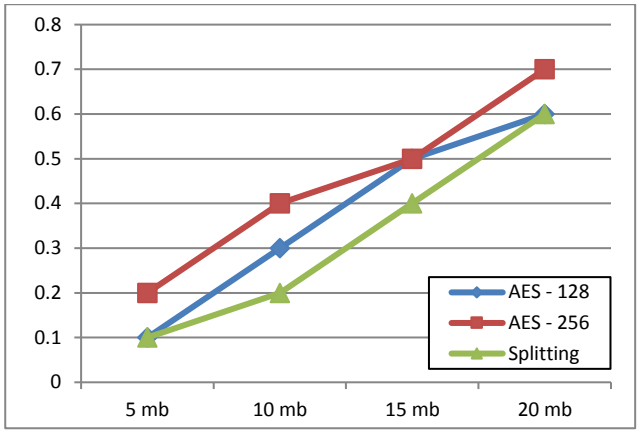


Fig 1: State chart diagram for Overall System

6. RESULT AND COMPARISON

For the implementation of our proposed work, we have created a web environment same as the user get in cloud. The user has an interface containing upload file and show file then he has to choose either upload the file or view their previously uploaded file. When the user selects the "Upload File" option, he has moved to the browser page where he has to choose the file from their local storage. After chosen the file, he also has to choose the respective security which he wants for the uploaded data, and accordingly encryption security will be provided to the data of user.We find out the time taken by the different options chosen by the user either it is general, secured or highly secured and compared them and find out the given result. We have used AES128 for general, AES256 for secured and file splitting for highly secured category.



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.

7. CONCLUSION

The Cloud Computing is the emerging technology and due to the increasing time, it also gets expanding. According to the time, the users in the cloud are also increases and with this major challenge is the security of the information stored in the cloud server. In our work we have discussed the security algorithms like TDES, AES-128/256 with the comparison between them. Also, we have introduced new security mechanism based on File Split. By go through all the results and graphs of the proposed work, we can conclude that our work is an efficient and effective secrecy-based system increases performance of the cloud environment and also reduces the processing time. Also, according the requirement of the information, they get that type of security. The framework shows that our proposed work provides the better security as compared to others.

As a part of the future work respective to our proposed work that this can be enhanced with better security algorithms like Asymmetric algorithm with better execution time, new techniques and methods used for providing better security to the information, other way data classification can also be used which enhance the system. Also, soft computing techniques can be used which provide the automatic data classification and better techniques for the confidentiality and integrity of the information.

REFERENCES

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

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

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

[4]. Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd Aldosari, "A Secure Cloud Computing Model based on Data Classification", Science Direct Procedia Computer Science 52 (2015) 1153 – 1158

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

[6] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853

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

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

[9]. Nasrin Khanezaei, Zurina Mohd Hanapi " A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia

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

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

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