INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Security Model for Cloud Computing by using Data Classification Methodology

Pankaj Pali
Student, Department of CSE, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India
Saurabh Sharma
Faculty, Department of CSE, Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

Abstract:
In Cloud Computing data is stored in the remote server and user access their data from the server. As increasing years, users on the Cloud also rapidly increasing and more users are deploying their data on the cloud. So storing data in the trust of 3rd party is mainly focus on the privacy and security of Data. Data can be a financial transactions, personal documents or files, multimedia etc. in cloud security is still a major concern. So existing solution for the problem is classifying the data and provide encryption according to that. The proposed framework is classifying the data according to its sensitiveness and for different category of data this framework provides different authentication technique and according to the level of sensitiveness it also provide required protection scheme. As compared to other solutions for the problem of security to the data present on the Cloud, this framework is more secure as it provides different level of authentication also. The data present on the cloud is secure by two ways firstly by the Encryption which is basic element of providing security and secondly with Authentication scheme.

Keywords: *Cloud computing, cloud storage security, data classification*

1. Introduction

Now a day cloud computing is the area which is continuously growing with huge amount of new technologies. One of the concept in the cloud computing is Cloud Storage. Cloud Storage is nothing but the space which is provided by the organization to the user to save their data on the remote server. People are more aware of the Cloud Storage currently and because of the advantages of the cloud members in the cloud are increasing every year. User can upload there data at any time and can access their data from anywhere by devices like Mobile, Laptop and Computer. Data is the vital assets of the user and it can be in any form like images, documents, any transactions etc. figure 1 shows us the different Cloud Providers organizations.

Data is the vital asset of the users. When the users deploy their data on the cloud the crucial issues which comes is the security and privacy of the data. Cloud Providers are responsible for the security of the data. Data deals with some of its properties like accuracy, validity, reliability etc.

In cloud computing the security of the data is mainly deals with basic security issues Confidentiality, Integrity and Availability. Data Confidentiality consists of privacy of the data. Integrity means it deals with the content of the data. Availability of the data means proper storage of the data that can be recovered in failure conditions.

Figure 1: Cloud Storage providers

In the Cloud Storage the main problem is in terms of security. In cloud data uploaded by the users is considered in the same way means all the data without considering the importance of the data high level security is applied to all the data. By using this concept there is the wastage of the time, performance also degrade. So the solution for this problem this paper is proposing a framework.

2. Related Work and Existing Solution

Cloud Storage has many benefits and great advantages. Some of the advantages are like provide better accessibility, one can easily access their data from anywhere by using Internet. Another benefit is we should not take the hardware storage with us for the data it also enhances the team work because one can easily be share their work and a group can collaborate with each other easily and many more advantages. Beside all the benefits and advantages of the Cloud there are some of the limitations of the Cloud. The limitation discuss in terms of public cloud. In the public Cloud the data stored in the cloud is visible to all or accessible to all and one can easily get the data because in public cloud data is open to the public.

Author in [1] proposed a benchmark for the transmit of the data. Here protection of the data during migration through benchmark is discussed for the Encryption overhead and security. For more security, more powerful encryption is required. Author in [2] discuss among threats involved in insecure APIs are anonymous access and/or reusable tokens or passwords, clear-text authentication, improper authorization and API dependencies. In the paper [3] the author proposed the new version of AES-512 bit encryption algorithm. The author presents the architecture for AES-512 and efficient hardware that requires to implementation of the Algorithm is also discussed. In this paper the author uses the 512 bit key size and same bit block size also uses which makes the algorithm more resistant towards the attacks. According to the user this algorithm provides the more security to the data with more throughputs.

The author in [4] studied the security as a part of survey. According to the survey of the author various other security issues should also be considered beside the main issues and their solution also. Here different data security concerns are analyzed and solved by classification of the data. Different security and protection is provided according to the degree of values of the data.

In [5] the author consider the two problems Confidentiality and privacy of the data in cloud. To overcome these two problems they design the framework which solves the problem of unauthorized access. Different mechanisms are used for different task like Key Management mechanism, Data Encryption mechanism, Multi-way Tree index mechanism etc. These mechanisms are different in client and the server side.

An effective security is achieved when the users is aware of the state of the data [6]. Data exists in one of the three states: at rest, at process and in transit. In the paper author convey that in all the three states data require different security. All the three states require different and unique security protection. For example if the data is considered as sensitive then it remains sensitive in all the states i.e. at rest, at process and in transit.

As the use of the cloud increases different algorithm are proposed for the protection of the data. In [7] author proposed an optimized technique for the security of the data by using encryption process. Here symmetric block cipher algorithm (CHis-256) to protect the data in the efficient manner. In the paper [8] the author shows us the efficient manner of the implementation of the AES-512 algorithm with proper and efficient utilization of the resources used in it. Here the comparison between the AES-128/256 and AES-512 is done and shows us the reasons to use AES-512 for more security with better throughput.

There are several types of issues [11] that cloud users face and consumer may face during the use of the services of the cloud. Most of the issues are with security to the data. The data is confidential and available when it is business. In paper [12] data classification technique is used for providing security to the data. Here the classification is done on the basis of the confidentiality of the data and according to the respective domain of classification security provided. Classification levels are Basic level, confidential level and High Confidential level. Here the best security technique which is used for the security is AES-256 with SHA.

Before applying security to the data it is important to understand and identify the various security challenges which are going to be faced. In [11] the author shows us the different security challenges other than the basic security issues. Here not only the author displays the security challenges but also focus on the percentage of importance of that challenges in the cloud computing. Some of the challenges this paper focus are security and privacy, Data leak prevention, Threat and Vulnerability management etc.

3. The Proposed Model Based on Data Classification

Our target is to implement proper solution for the above mentioned problem. For the solution to the problem we have to handle two issues user encounter when using cloud services. They are the users concern about the unauthorized access to the data i.e. Hacking of the data and the other one is infeasibility of the security provided to all the data without consideration of the importance or sensitiveness of the data.

Let us take an example suppose we have 100 GB data which is uploaded by the user in the space provide by the some cloud storage providers. Out the 100 GB data only 15% of the data is which requires more attention or we can say that data need high security and data other than 15% contains basic and moderate data combined. So it is not feasible to implement all the data with top level security as that only 15% required this. Other get unnecessary high security instead user also knows that data is not so important. So we are proposing the security model which works on the methodology "Classification of the Data". Data Classification is the process which categorizes the user's data into some of the sets. The Classification can be done with many ways like according to confidentiality of the data, according to the storage, their formats, their usage etc. Here we are considering the sensitiveness of the data and differentiate data according to it. We are categorizing data into 3 different level say General Level, Sensitive Level and Unrestricted Level.

Figure 2: Classification of Data

3.1. Methodology Details

The different security levels proposed in this framework
Model is shown in the figure 2.

- Basic Level: The basic security level concerned with the general type of data like photos, videos etc. which do not need high degree of sensitiveness. So this level the security is basic security which is used by most of the product online. For that we use Triple DES encryption technique for the encryption and also Single Factor Authentication scheme for the authentication to the data.
- Sensitive Level: Sensitive level is designed for the data with medium sensitive degree like personal files, videos, pictures, documents etc. In this level we are going to use AES-256 encryption scheme. It means data which belongs to this level will be secure by the Advance Encryption Standard (AES) with the key size 256 bit. And also different authentication technique is also proposed i.e. Multifactor Authentication.
- Restricted Level: The other level of security is Restricted Level. All the data which the user wants to be highly secure are comes under this category. Data like Financial Transaction, Secret documents of organization; Military data etc. all comes under this. Here also in this level Multifactor an authentication technique is used.

Security level	Authentication	Encryption
Basic level	Single Factor	Triple DES
Sensitive level	Multi Factor	AES-256
Restricted level	Multi Factor	AES-512

Table 1: Proposed Model scheme

3.2. Technology Details

In this section we will discuss the techniques used in this framework for the Encryption as well as for Authentication. As we already told that we are going to use 3 security techniques: Triple DES, AED-256 and AES-512.

a) Triple DES: Data Encryption Standard is the symmetric block cipher develop by IBM. Triple DES was created back when DES was getting a bit weaker than people were comfortable with. So we can call Triple DES is EDE (encrypt, decrypt, encrypt). The working way of this technique is you take three 56 bit key and encrypt with key1, decrypt with key2 and finally again encrypt with key3. Triple DES has two-key version and three-key version. In two key version two keys are same while one is different. And that of three-key version all the keys are different.

b) AES-256: Advance Encryption Standard (AES) is a symmetric block cipher and is implement in software and hardware throughout the world to encrypt the sensitive data. AES uses the symmetric ciphers means the same key is used to for encrypting and decrypting the data. So both the sender and receiver has to know the secret key. There are 14 rounds for 256 bit key. Each round consists of several processing steps that include submission, transposition and mixing of the impute original text and transform it into the final output of cipher text.

c) AES 512: In AES-512 bit key encryption there are 14 rounds and each rounds consists of several step as mentioned in AES 256.

Now we are already discuss that with the several security techniques we also provide different authentication for each category or security level.

a. Single Factor Authentication: As the name of the authentication shows that single factor means only one factor is responsible for the authorization of the valid user. It means "that the users know". Single layer of security is provided in this scheme. The most reorganized type of single factor is password protection. All the username and password protection to the data is comes under Single factor authentication techniques.

b. Multi Factor Authentication: As the name of the authentication techniques shows that it is two factor means two factor is responsible for the protection of the data. It is the advance version of the Single Factor. In addition to the Single Factor user

has another factor for checking of the authenticity of the user. Examples of the Two Factor Authentication are as follows: Two Step Verification, OTP (One Time Password) is also lies on this category of authentication.

4. Conclusion

In our framework we have applied the techniques which provide the best solution to the basic problems of users i.e. Violation of Integrity by Unauthorized access of data and Confidentiality of the data. We have used Single Factor and Two Factor Authentication techniques for integrity of the data and Triple DES, AES-256 and AES-512 algorithm for the Encryption of the data for achieving the confidentiality of the data. As a part of the future work a Hybrid Encryption techniques can be used and the classification of the data can be done automatically by applying the proper mechanisms.

5. References

i. Ji Hu and Klein A, "A Benchmark of transparent data encryption for migration of web application in cloud", 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, 2009
ii. CSA, "Top Threats to Cloud Computing V1.0," 2010
iii. Abidalrahman Moh'd, Yaser Jararweh, Lo'ai Tawalbeh "AES-512 : 512 Bit Advanced Encryption Standard Algorithm Design and Evaluation" Seventh International Conference on Informatin Assurance and Security (IAS-2011)
iv. Rizwana Shaikh and Dr. Sasikumar, "Security Issues in Cloud Computing: A survey. International Journal of Computer Applications 4-12 April 2012.
v. Yang Wei, Zhao Jianpeng, Zhu Junmao, Zhong Wei, Yao Xinlei "Design and Implementation of Security Cloud Storage Framework" Second International Conference on Instrumentation and Measurement , Computer, Communication and Control-2012
vi. Frank Simorjay, "Data Classification for Cloud Readiness", Microsoft Trustworthy Computing Doc. 2014
vii. Jararweh, Yaser, Ola Al-Sharqawi, Nawaf Abdulla, Lo'ai Tawalbeh and Mohammad Alhammouri, "High-Throughput Encryption for Cloud Computing Storage System", International Journal of Cloud Applications and Computing (IJCAC) 2014
viii. Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya and Mahesh Sanap "AES Algorithm Using 512 bit key Implementation for Secure Communication" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014
ix. Anup Mathew, "Survey Paper on Security & Privacy Issues on Cloud Storage Systems", EECE, Term Survey Paper, April 2012
x. Dr. L. Arockiam, S. Monikandan "Efficient Cloud Storage Confidentiality to Ensure Data Security" International Conference on Computer Communicaion and Informatics (ICCCI)- 2014.
xi. Rizwana Shaikh and Dr. M. Sasikumar "Data Classification for achieving Security in Cloud Computing" ; 493-498
xii. R. Velumadhava Rao, K. Selvamani "Data Security Challenges and Its Solution in Cloud Computing" International Conference on Intelligent Computing, Communication and Convergence (ICCC-2015)
xiii. Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd Aldosari "A Secure Cloud Computing Model based on Data Classification" First International Workshop on Mobile Cloud Computing Systems, Management and Security (MCSMS-2015).