ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Secure Model for Cloud Computing by using Data Classification Methodology

Radha Patel, Satish Dehariya

M.Tech Student, Dept. of Computer Science Engineering, Samrat Ashok Technological Institute, Vidisha (M.P.), India

Assistant Professor, Dept. of Computer Science Engineering, Samrat Ashok Technological Institute, Vidisha (M.P.), India

ABSTRACT*:* In cloud computing data stored in the 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. The main concern regarding data when it is stored in the trust of 3rd party, is Security and Privacy of the data is very important. Data can be a financial transaction, 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 provides encryption according to that. The proposed framework is classifying the data according to its sensitiveness and 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 others solution for the problem of security to the data present on the Cloud, this frame work is more secure as it provide different level of security and authentication scheme. The data present on the cloud is secure by two ways firstly by the Encryption which is the basic element of providing security and secondly with Authentication scheme.

KEYWORDS: Cloud Security, Data Classification , Cloud Computing.

I. INTRODUCTION

Now a day's Cloud Computing Technology is the most emerging Technology comes in the real world [1]. Users are more aware of the benefits of the Cloud Computing and they are using it. Cloud Computing is the next generation system which provides an easy and customize way of managing data in the Internet. It provides various services for accessing the data and work with the application of Cloud to the user. Users can upload their data in the Cloud Storage and can access through anywhere through any devices like Laptop, Desktop, Mobile. Data is the vital assets of the users. Data can be in any form like documents, videos, photos etc. Whenever the discussion of data comes, some of the properties of data emerges. Some of them are Accuracy, Completeness, and Consistency etc. Data in Cloud is mainly deals with 3 security issues confidentiality, integrity and availability. Data Confidentiality means data should be confidential to others. Unauthenticated or Unauthorized users can't be able to access or use the data. Data Integrity means content of the data should not be violated. To achieve data integrity consistency and accuracy of the data should be maintained. Availability means data should be available always when the users want to access their data. For achieve the Availability of the data proper storage type, proper recovery and backup management has to be implemented [5]. Data Classification means categorizing the data into number of levels. For security of the data in Cloud Classification used in a way that the users Data is categorized into several level and according to the importance of data in the respective level security is provided[2]. This is the best approach towards the security mechanism in Cloud Computing because instead of providing same level of security we just differentiate the data and according to their needs we secure that data. Classification of the data can be done with many ways like according to the sensitiveness, according to storage, according to type of data, content of the data etc. As we know data is very crucial in service delivery model. So we analyzed the data on the basis of sensitiveness and according to sensitivity we provide Level of Authentication and Security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

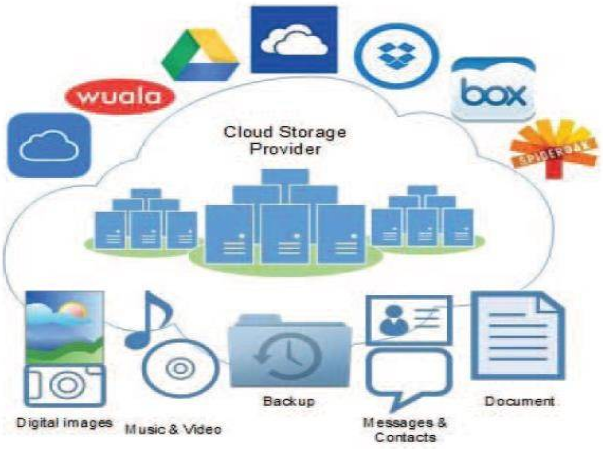

Fig1 Personal cloud storage

As above are the various cloud storage providers which provide space to the user to put their crucial data in the cloud and the provider has the responsibilities for the protection of the data [7]. The protection of the data is done by the encryption of the data. Different Cloud Service providers are using different techniques for the protection of the data [11].

II. LITRATURE SURVEY

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.

Ji Hu and Klein A 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. In the paper[3] the author proposed the new version of AES-512 bit encryption algorithm[1]. 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 throughput.

Rizwana Shaikh and Dr. Sasikumar 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 [4]. Different security and protection is provided according to the degree of values of the data.

Yang Wei et al consider the two problems Confident-iality and privacy of the data in cloud[5]. 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.

Frank Simorjay considered that 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

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.
Jararweh et al 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.
Lo'ai Tawalbeh et al provided the 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.
R. Velumadhava Rao, K. Selvamani gave the details of 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 securitychallenges 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.

III. PROPOSED WORK

In this paper our target is to handle two basic issues users are facing during the deployment of their data over the cloud. First one is the unauthorized access to the data by the intruders or hackers and second one is the infeasibility of encrypting all the data without any categorization. So we propose a framework for solving the above mention problems. The proposed framework allows the users to Authenticate and Encrypt the data according to its classification. But the classification of the data can also be done in many ways like according to storage, content of data, how the data accessed and so on.
For example suppose we have a 100GB which are going to deploy over the Cloud and out of which 15% of data is sensitive which require more security. So encrypting the whole data with same level of security and with same key size encryption then it is not feasible in terms of processing time because it takes more time and except for data other than 15% is waste of time.

A. AUTHENTICATION : Generally authentication consists of mainly two parts – Username and Password. Username of user ID is to identify the user and password or token is to confirm that the user is valid user.

B. AUTHORIZATION : Authorization provides an authenticated user the ability to access their data, application of the cloud, data files or some other materials. It assigns the user proper rights over the data, right to use, modify or delete. Successful authorization requires proper mechanism which is well enough to validate the individual users and the role of the users. With the role and access controls of the users there should be a policy which confirm that which data is seen by which user and which not, then we can say that proper authorization system is made.

C. ***ENCRYPTION :*** This is the mostly used ultimate solution of achieving the security to protect data. Converting the original text or data into a unreadable form is best for the security so that no one can know what is written. Best level of Encryption techniques are discussed in the related work which is now a day's using in the real world.

Our proposed framework will classify the data into different security level according to their sensitiveness into three level Basic Level, Sensitive Level and Highly Confidential Level. Different Authentication techniques are used in this framework like Single Factor and Two Factor Authentication. Similarly different security techniques are used to different level like AES-128, AES-256, and AES-512.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A. FRAMEWORK DETAILS:

The Security level in our work is according to the sensitiveness of data and the levels are Basic, Sensitive and Highly Confidential.

- Basic Level : The basic level of security is mainly concern the basic data like videos, photos etc. All the data which the user consider as general are comes under this category. Here for basic level we provide basic security or low level of security like AES -128 for Encryption with Single Factor Authentication.
- Sensitive Level : Sensitive Level is the another level of security in which the data which is personal data to the user is reside in this category. All the personal files, videos, pictures, documents etc. are the sensitive data and associate with this level. For the Sensitive Level we provide medium level of security like AES-256 for Encryption with Two-factor Authentication.
- Highly Confidential Level : The data which is very sensitive or confidential according to user are comes under this category. For the Highly Confidential data top level of security is provided like AES-512 for Encryption with Two-Factor Authentication.

Security Level	Authentication	Encryption
Basic	Single Factor	AES-128
Sensitive	Two Factor	AES-256
Highly Confidential	Two Factor	AES- 512

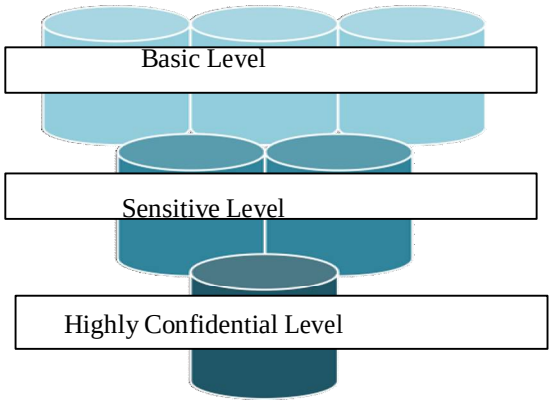

Fig.2 hierarchy of confidential level

In this framework we have discuss that we are not only provide Encryption technique according to the classification but also we provide the Authentication. Here we are using two category of Authentication First one is Single Factor Authentication and other one is Multi Factor Authentication.

B SINGLE FACTOR AUTHENTICATION:

As the name of the authentication shows that single factor means only one factor is responsible to validate the user. It means “that the user knows”. Single layer of security is provided in this scheme. The most recognized type of single factor is password. In the username and password the password is the factor which makes a single layer of security.

C. TWO FACTOR AUTHENTICATION:

As the name of the authentication techniques shows that it is two factor means here two factors are 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. Two Factor authentication such as two step verification. Also One Time Password is also a second factor for the authentication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

IV. PROPOSED ALGORITHM

A. AES-512

AES 512 is a new version of the Advanced Encryption Standard (AES) algorithm. The new algorithm (AES-512) uses input block size and key size of 512-bits which makes it more resistant to cryptanalysis with tolerated area increase. AES-512 will be suitable for applications with high security and throughput requirements and with less chip area constrains such as multimedia and satellite communication systems. AES-512 show tremendous throughput increase of 230% when compared with the implementation of the original AES-128.

AES-512 ARCHITECTURE

The top level architecture of the AES-512 bits is shown in Figure 1. The plaintext and the key size are 512-bits each (organized in bytes). The AES-512 algorithm processes the data in 10 rounds. The key and the input data are loaded when the Loadkey control signal is one and zero, respectively. The Encrypt signal starts the encryption process, while reset resets everything to zero. The resulting cipher text is also 512-bits. More details about each of the transformations used in the AES-512 are described in the coming subsections. Where the key expansion procedure is explained later since each round needs its own key generated according to this procedure.

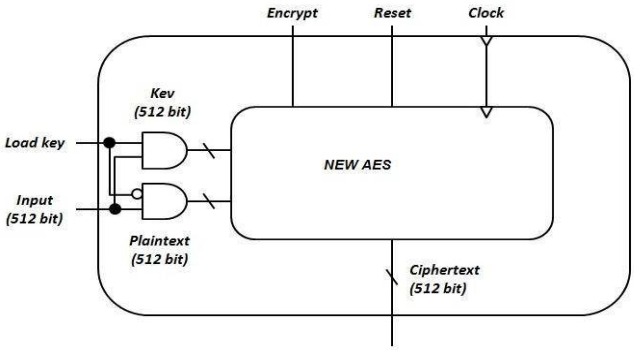

Fig.3 Top level of architecture AES-512

B. AES-128/256

AES stands for Advance Encryption Standard is the advanced version of DES and this the Symmetric key algorithm means similar key is exercised for the encryption and decryption of the information. In AES 128/256, the key size is either 128 bit or 256 bit depends upon which algorithm used by the user which encrypt the block of file. Each block is of 128/256 bit in size. AES is six time faster than the TDES. The main reason for the replacement of the TDES is that the key size is too small and another is for provide Strong security

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

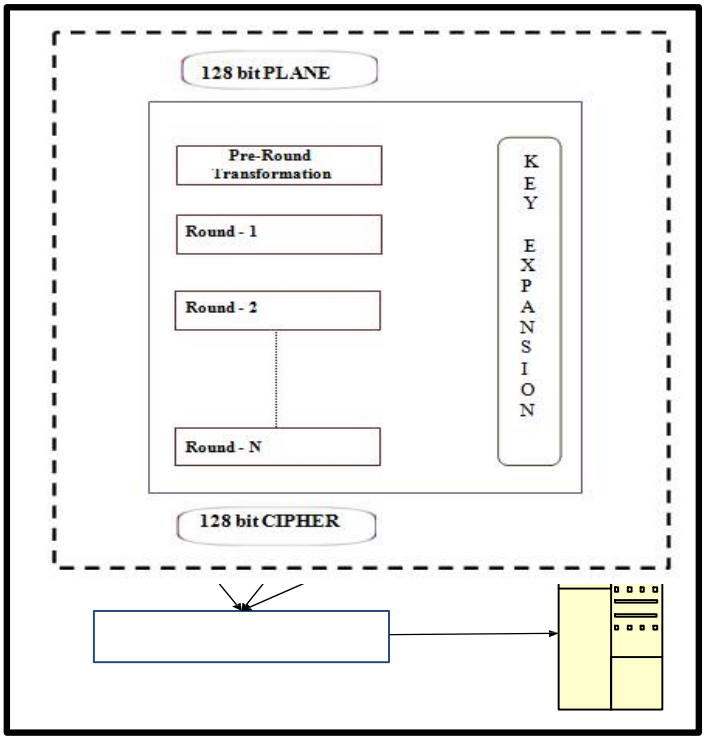

Fig. 4 AES- 128 Encryption process block diagram

C. FILE SPLITTING

In our proposed work we have used a concept called File Splitting. File Splitting is the technology or mechanism which divides the particular files into chunks. Here chunks are used for denoting the small parts of files. So the chunks are then stored in different location and when that file is required then all the chunks from their location fetched up and merged to form the original file. The main importance of the file splitting is to increase the execution time. The situation the file splitting is going to be a good option where execution time important factor as splitting file into chunks and execute each chunks may reduce the processing time.

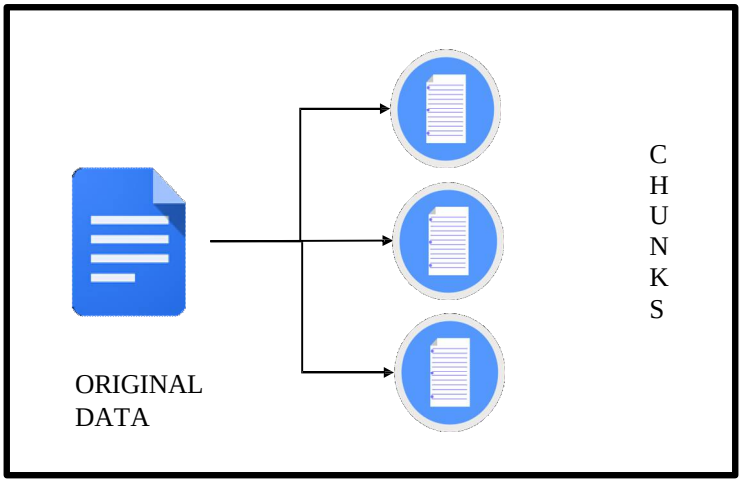

Fig. 5 File Splitting

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

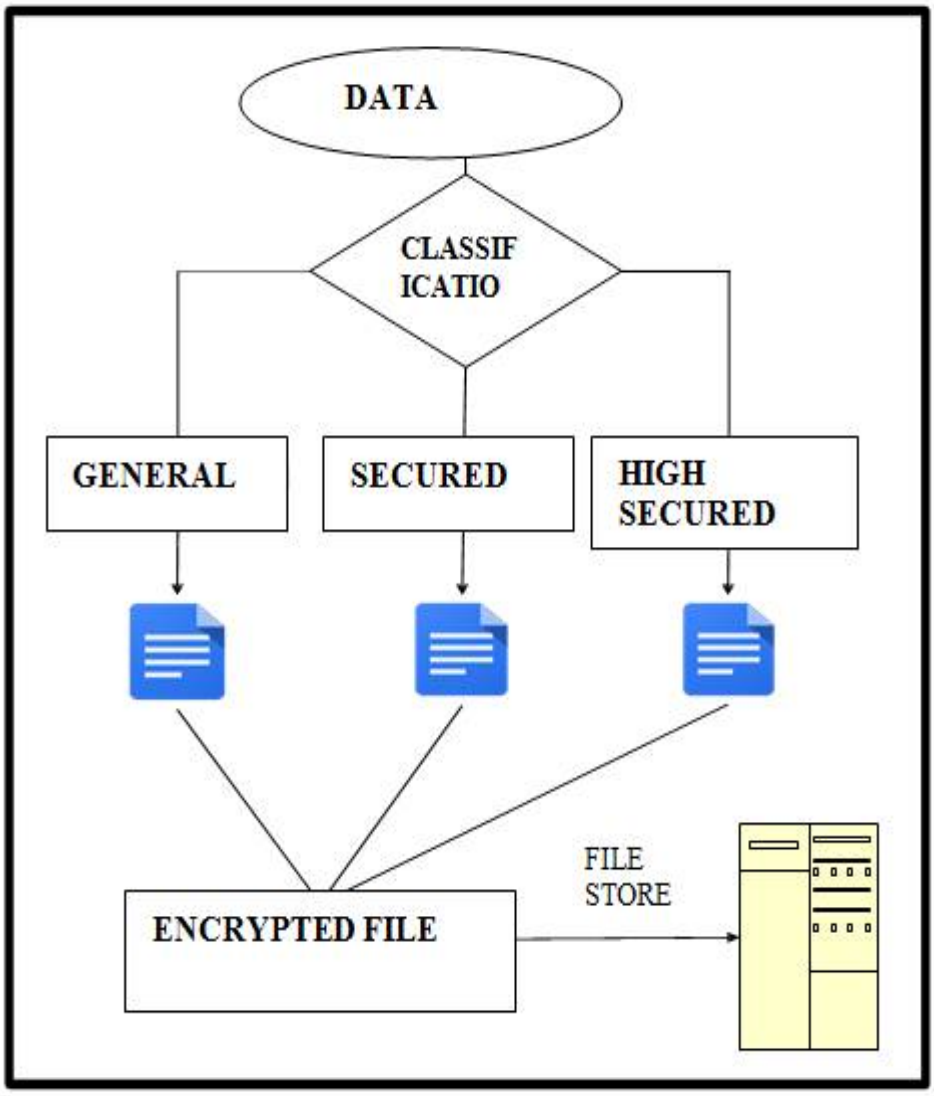

Fig .8 Flow Chart of Proposed Work

V. RESULTS AND ANALYSIS

The simulation results show the analysis and performance in different symmetric algorithms. The algorithm AES-512, performance of proposed system, which is based on File Splitting Concept, is better as compared to existing algorithm AES-256.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

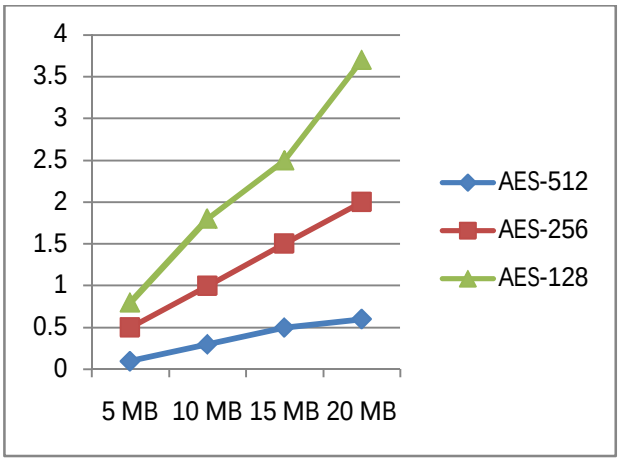

Fig.6 Evaluation of the security algorithms

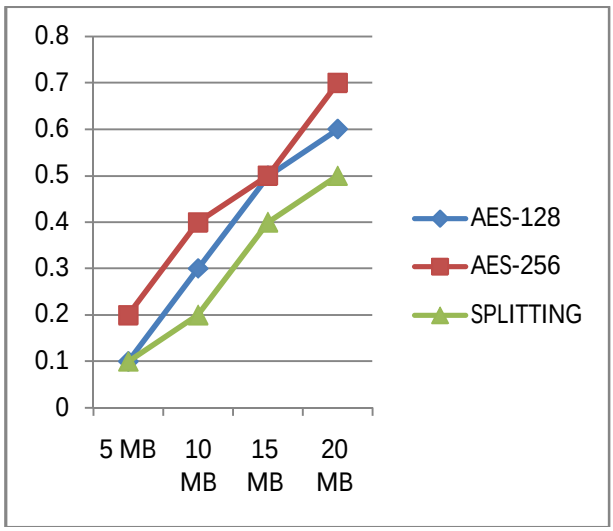

Fig.7 Average time taken by Encryption Algorithm (in ms)

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

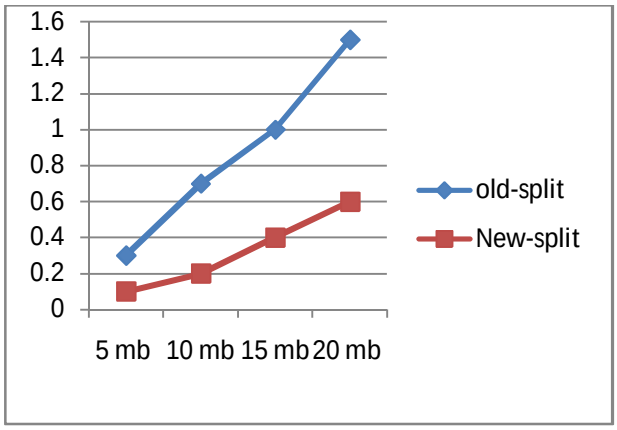

Fig.8 Average Time Comparison between Old Split and New Split Scheme

In the following graph we have used two terms called Old Splitting and New Splitting. In the Old Splitting we consider the three security algorithm to encrypt the chunks i.e. AES-128, AES-256 and Triple DES while in the New Splitting we only use two security AES-128 and AES-256. According to our comparison, we can clearly see in the graph that using TDES security, the encryption time becomes more and without it, it works well. So this is the reason we have used the New Splitting concept in our work.

Table .1 Comparison between Existing System and Proposed System:

Comparison Factors	Existing System	Proposed System
Security	In existing system, high level security is AES-256 security algo.	In our work, for high security we used File Splitting Concept which is more secure than AES-256.
Drawback	In existing system, there is a drawback that they are using AES-256 for low level security and AES-128 for moderate level security which is inappropriate to Data Classification Scheme.	In our work, we have provide the low security to low level and high security to moderate level which is feasible with the Data Classification Scheme.

VI. CONCLUSION AND FUTURE WORK

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 Hybrid Encryption techniques can be used and automatic classification of the data with proper algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

REFERENCES

[1] 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.
[2] CSA, "Top Threats to Cloud Computing V1.0," 2010
[3] Abidalrahman Moh'd, Yaser Jararweh, Lo'ai Tawalbeh "AES-512 :512 Bit Advanced Encryption Standard Algori-thm Design and Evaluation" Seventh International Conference on Informatin Assurance and Security (IAS-2011).
[4] Rizwana Shaikh and Dr. Sasikumar, "Security Issues in Cloud Computing: A survey. International Journal of Computer Applications 4-12 April 2012.
[5] 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.
[6] Frank Simorjay, "Data Classification for Cloud Readiness",Microsoft Trustworthy Computing Doc. 2014.
[7] 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.
[8] 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.
[9] Dr. L. Arockiam, S.Monikandan "Efficient Cloud Storage Confidentiality to Ensure Data Security" International Conference on Computer Communicaion and Informatics (ICCCI)- 2014.
[10] Rizwana Shaikh and Dr. M. Sasikumar "Data Classification for achieving Security in Cloud Computing"; 493-498.
[11] R. Velumadhava Rao, K. Selvamani "Data Security Challenges and Its Solution in Cloud Computing" International Conference on Intelligent Computing, Communication and Convergence (ICCC-2015).
[12] 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).
[13] Fara yahya, Robert j Walters , Gary B Wills."Protecting Data in Personal Cloud Storage with Security Classifications". Science and Information Conference
[14]. V. Sreenivas, C. Narasimham, K. Subrahmanyam, P. Yellamma, " Performance Evaluation of Encryption Techniques and Uploading of Encryped Data in Cloud", 4th ICCCNT-2013.