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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

Information Protection Using Data Classification Procedure in the Cloud Computing

Sakshi Nema, Prashant Kumar Koshta

Research Scholar, Department of Computer Technology & Applications, Gyan Ganga College of Technology Jabalpur (M.P.), India

Professor, Department of Computer Science & Engg, Gyan Ganga College of Technology, Jabalpur (M.P.), India

ABSTRACT: Data classification is broadly characterized as the way toward sorting out information by important classes with the goal that it might be utilized and secured all the more proficiently. It additionally takes out numerous duplications of information, which can diminish capacity and reinforcement costs, and accelerate the pursuit procedure. In the distributed computing framework, the issue is that the specialist co-ops treating every one of the information in a similar way implies they give basic security to every one of the information for the specific client without considering that whether that required that security or not. So as an answer for this issue, we proposed the idea of information order. In our proposed work, we order the information into classifications in view of the mystery of the information and specific classification of the information is secured with particular level of security. At times, information order is an administrative necessity, as information must be accessible and retrievable inside indicated time spans. For the motivations behind information security, information characterization is a valuable strategy that encourages legitimate security reactions in light of the kind of information being recovered, transmitted, or duplicated using AES-128, AES-256 and 3DES as encryption algorithms. User's private key is also used in encryption algorithms for better security of data. Utilizing our proposed work information which required high security they get high, and which need low security they get low. This work is more secured and productive than alternate works done as such far.

KEYWORDS: Cloud Computing, Encryption, Data Classification, AES128, AES256, 3DES, Private Key, Data Security

I. INTRODUCTION

II.

As web keeps on developing with time, it is required for security conventions and strategies to refresh too so clients and associations keep on enjoying its advantages without being worried about any kind of dangers. Yet, as number of hubs increments from millions to presumably billions the danger of malware, spam and infections has just expanded. In this way, it's compulsory to manufacture strong frameworks which can deal with interruption location as depicted in and accordingly kill any risk emerging out of botnets, malware or spam. Besides, investigate has been led in the territory of information concealing methods as depicted in to decrease the encryption overhead experienced by the framework and in addition in the area of anticipating listening in by with the assistance of spread range adjustment as specified. Confirmation is one such part of web security which if ignored enables unapproved clients to get to frameworks and take information. Be that as it may, with aggressors accessing refined advancements, the requirement for multi-factor validation has come up and how it can be conveyed in different frameworks is portrayed. Validation to a framework has dependably brought about overhead for the frameworks and deferral for the end clients. Along these lines, a great deal of exertion in the course of the most recent decade has been attempted to address this issue.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

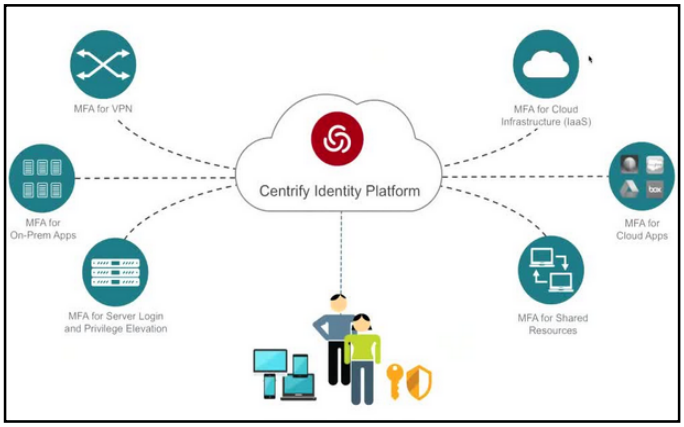


Figure 1.1 General Web Architecture

As it were the ease of use of a framework must increment if the client means to utilize it once a day. The ease of use of a framework is estimated utilizing five variables: speed, proficiency, notice capacity, learns capacity and client inclination. Speed is worried about how rapidly validation can be refined and effectiveness is about how often framework can be to blame to verify wrong substance Then again, learn capacity infers that it is so natural to arrange the framework with a specific end goal to verify oneself and notice capacity shows that once realized, that it is so natural to validate in the framework in future. At long last, the client inclination considers the client's decision of confirming the framework gave it's sheltered. While confirming it's essential to consider an exchange off between the previously mentioned factors. Multi-factor validation is a security framework, which contains in excess of one type of verification framework executed to check a client's personality. For instance, this framework could contain biometrics, tokens/savvy cards, or secret key based validation arrangements. By utilizing the blend of these distinctive validation frameworks, the verification procedure will end up more grounded, and the security will get improved. The initial segment of proposal is concentrating on multi-factor validation innovations and business issues, seeing accessible verification arrangements which could bolster and be coordinated into multi-confirmation structure. A choice will be offered after the examination of the vast majority of the confirmation frameworks. At last we pick Keystroke Dynamics and Ranking secret word as our validation frameworks. Multi-factor verification is the way toward recognizing an online client by approving at least two cases introduced by the client, each from an alternate classification of components. Factor classifications incorporate information (something you know), ownership (something you have) and inherence (something you are). Today, most shoppers and specialists utilize a watchword to increase online access to their records and systems. They regularly utilize a similar secret word for numerous records, share passwords, and abuse them in different ways, bargaining security. Rather, utilizing at least two sorts of elements to give qualifications to online access, alluded to as "multi-factor confirmation," can give more grounded security.

II. TYPES OF DATA CLASSIFICATION

Data portrayal every now and again incorporates an extensive number of marks and names, describing the kind of data, arrangement, and its dependability. Availability is in like manner a portion of the time considered in data gathering shapes. Data's level of affectability is regularly gathered in light of changing levels of noteworthiness or mystery, which associates with the security endeavours set up to guarantee each request level. For example, an affiliation may describe data as:

1. Restricted
2. Private
3. Public

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

In this event, open data addresses the smallest sensitive data with the slightest security necessities, while restricted data is in the most astonishing security request and addresses the most delicate data. This kind of data game plan is routinely the starting stage for a few, tries, trailed by additional ID and naming frameworks that check data in light of its congruity to the endeavour, quality, and distinctive portrayals..

i . Restricted Data

Data should be appointed Restricted when the unapproved revelation, modification or devastation of that data could make a basic level of risk the University or its branches. Instances of Restricted data consolidate data secured by state or government assurance headings and data guaranteed by protection assertions. The most hoisted measure of security controls should be associated with restricted data.

ii. Private Data

Data should be designated Private when the unapproved exposure, change or destruction of that data could achieve an immediate level of peril to the University or its backups. As is normally done, every single Institutional Datum that isn't explicitly named Restricted or Public data should be managed as Private data. A sensible level of security controls should be associated with Private data.

iii. Public Data

Data should be designated Public when the unapproved disclosure adjustment or obliteration of that data would achieves basically zero danger to the University and its accomplices. Instances of Public data join official explanations, course information and research creations. While for all intents and purposes no controls are required to guarantee the security of Public data, some level of control is required to turn away unapproved change or devastation of Public data.

III. DATA PROTECTION LEVEL

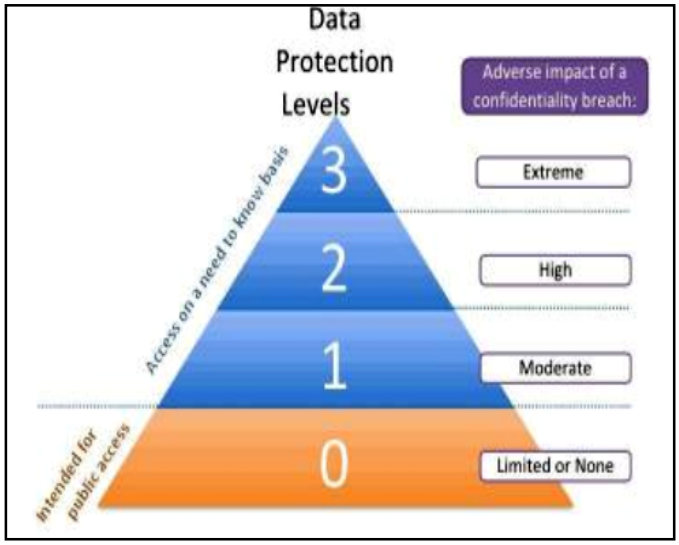


Fig 1.2 Data Protection Level

Protection Level 0 is held for data that would cause no (or obliged) unpleasant impact to the grounds if made open. Inventory data and other open information, for instance, course postings fall into Protection Level 0. (Note: Protection Level 0 excludes list information about understudies who have requested not to release their information. This decision

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

is recorded in Bear Facts, and should be checked before releasing registry information unless the understudies have given specific assent.

Protection Level 1 requires more protections and powers confines on sharing in light of the fact that the loss of grouping or trustworthiness of this data would realize guide unpleasant impact to the grounds. To secure individual security, information about individuals is named Protection Level 1 unless it is by and large appointed level 0, 2 or 3. Understudy data representations fuse transcripts, grades, exam papers, test scores, course enrolment, and evaluations. Furthermore, staff and insightful work compel records fall in protection level 1 unless recognized in various orders. Other information (not about individuals) that isn't proposed for open usage may similarly be protection level 1 data. While Protection Level 1 data or higher isn't gotten ready for open release it may regardless be at risk to open record, suit or other honest to goodness disclosure requests.

Protection Level 2 (high adverse impact) data consolidates "see enacting" data for which law powers excessive requirements if revealed dishonourably. This data should not be secured unless it is completely required and absolutely guaranteed:

- Social Security Number
- Driver's allow number or California Identification Card number
- Financial account number, credit or charge card number, in blend with any required security code, get the chance to code, or watchword that would enable access to a man's cash related record
- Personal helpful information
- Personal medicinal scope information

Protection Level 3 is required in select events of potential ridiculous horrible impact, for instance, systems that regulate accreditations for various immaterial however delicate structures. Most faculty and staff work with Protection Level 1 data in any occasion. You may similarly manage Protection Level 2 data in case you handle work power, prosperity or cash related trades. On the off chance that it's not all that much inconvenience review the Berkeley Data Classification Standard to adapt yourself with grounds game plan norms and how they apply to the different sorts of data you frequently use. If you have request with respect to data arrange, contact the data or system proprietor (that is, the individual who is essentially accountable for the data or structure).

IV. PROPOSED ARCHITECTURE

The Proposed secure dispersed handling model considering information approach, we will probably manage two issues the client experience while utilizing disseminated figuring associations. The first is client's worries over hacking dangers whether inside or remotely. The other one is the infeasibility of scrambling all information without thinking about its request degree. Hence, we propose a structure that enables the clients to encode their own data utilizing data divide, encryption and private key that isn't accessible for the others. What's more we scramble information bases on the level of riddle. Contemplating the level of insurance in social affair information would spare time and encode the less essential information with a key level of security rather than an extraordinarily riddle one. In this manner, we propose our ensured disseminated capacity exhibit that encodes information as indicated by its security degree through three levels: significant, riddle and unbelievably portrayed. The proposed strategy depends upon manual social event, which surmises that the client will exhibit the secret level of information. In the kill of this locale we will show our proposed structure in unnoticeable part. We in addition clear up quickly the information depiction design and show created by point of fact fathomed encryption and cryptographic checks like AES-128, AES-256 and 3DES which are utilized to guarantee riddle and reliability of information. Not with standing talking about the blueprint that we have facilitated to help us in building our system. Information portrayal is the methodology that licenses affiliations and people to arrange every specific sort of information and data resources as exhibited by its insurance degree, which will pick the level of security the information needs. Demand is made to ensure data affectability and a fitting security for the by-low secured data. Information can in addition be organized in perception to how as routinely as possible it must be gotten too.

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

4.1 Framework Details
The three security levels in the proposed indicate are appeared in Figure, key, private and essentially described.

Basic Data level: The essential level is worried in scrambling a general kind of information that needn't dawdle with an unusual condition of request. Henceforth, this level offers a key level of security and is utilized by a generous fragment of the things accessible on the web. For that, we propose utilizing default security for scrambling the correspondence between the use of the customer and the server utilizing HTTPS. The HTTPS gives fundamental secure correspondence confirmation between clients on the web. At the requested level we utilize AES-128 and AES-256. This encryption plan scrambling figuring with an altered piece size of data which is isolated in two areas.

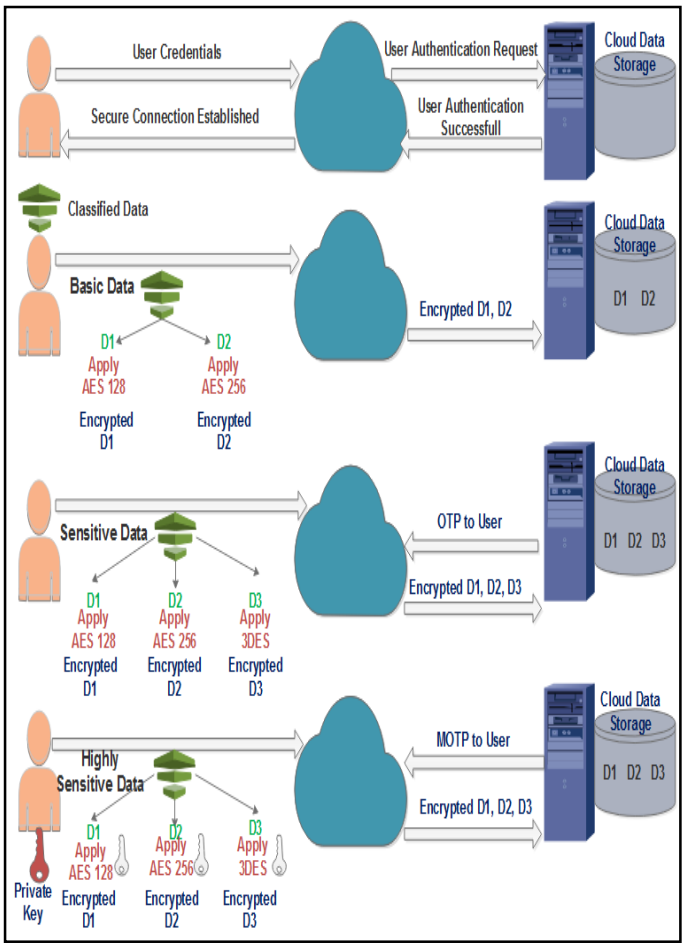


Fig.1.3 The proposed secure cloud framework

Sensitive Data Level: Confidential level is proposed for information with medium puzzle degree. In this level, the encryption is done at the customer side i.e. it depends upon customer side encryption. At the requested level we utilize AES-128, AES-256 and 3DES. These encryption designs scrambling estimation with a balanced piece size of data which is isolated in three segments.

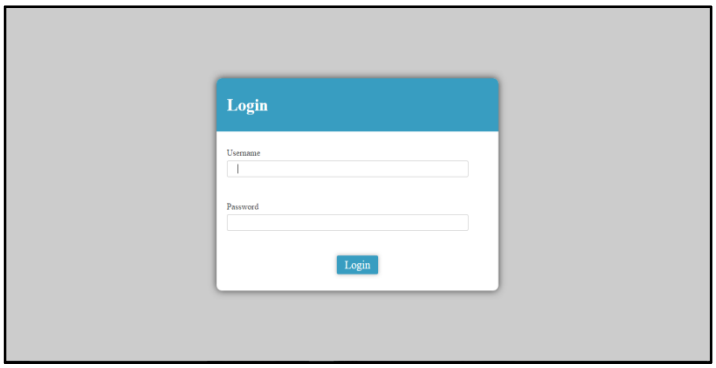
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

Highly confidential level: This level handles the most pivotal information, for example, money related exchanges and military data. Clients are particularly worried over losing this sort of information and still shun utilizing all the new offered associations in light of the high assurance of the information and the request he may have. Along these lines, at this level of security the client is furnished with an anomalous condition of portrayal and uprightness by utilizing two suggested figurings. The AES-128, AES-256 and 3DES encryption estimation with the help of using customer's private key is used for encoding top-sensitive information with a specific extreme target to frustrate unapproved get to.

VI. RESULTS

1. Login Page which will access by the cloud user for the login to their account.



ig 1.4 User Login Page

2. After successful login in the user get the Home Page where the user have to choose one option either to upload the data or to view the data present in his account.

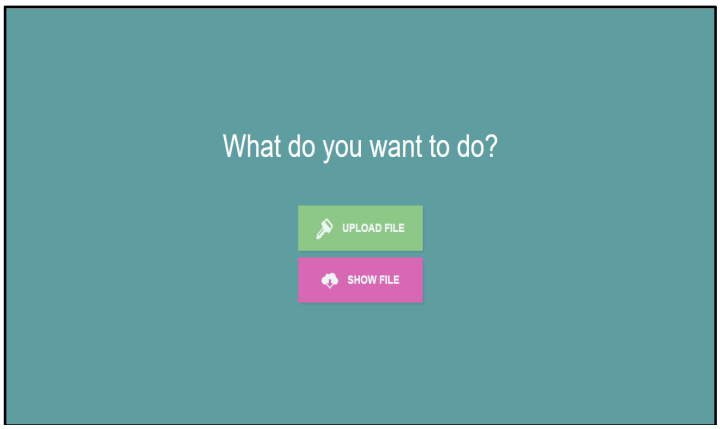


Fig 1.5 User Data Upload Page

3. When the user choose “Upload File” option for uploading the file, he redirect to Uploading Page where user choose the file and level of protection for that particular file.

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

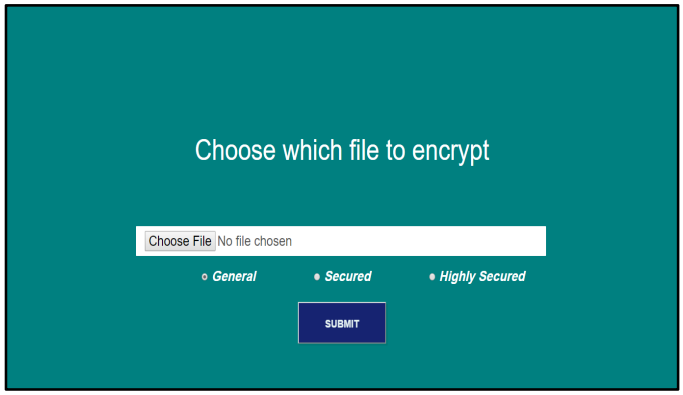


Fig 1.6 User Data Selection Interface for Upload

4. After the successfully uploading data in the cloud the user again redirects to Home Page and choose "Show File" to display the data and redirect to Display Page.

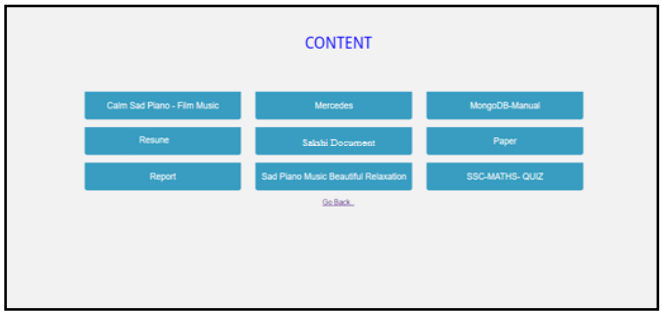


Fig 1.7 Showing User's Data in Cloud Storage

VII. COMPARISON

As a part of the implementation, initially we have tested the performance of the symmetric encryption algorithms including AES-128, AES-256 and 3DES before choose the algorithms for the respective category. To evaluate the performance of the algorithms we have find out the execution time of each algorithm with different data size. In our work, we have done evaluation based on four different data size i.e. 5mb, 10mb, 15mb and 20mb. The selection of the different data size is random. By comparing, we get that our proposed approach has maximum efficient time as compared to Existing work done.

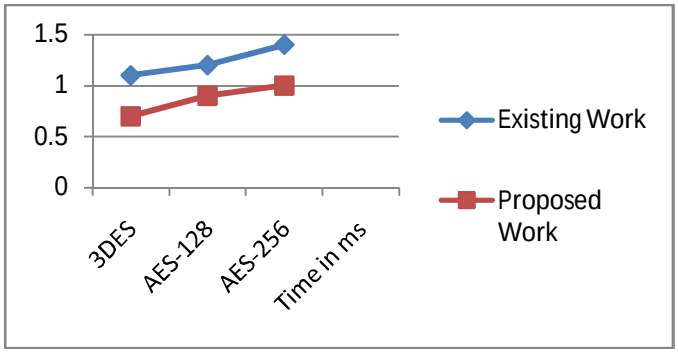


Fig 1.7 Average time taken by Encryption Algorithm (in ms)

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

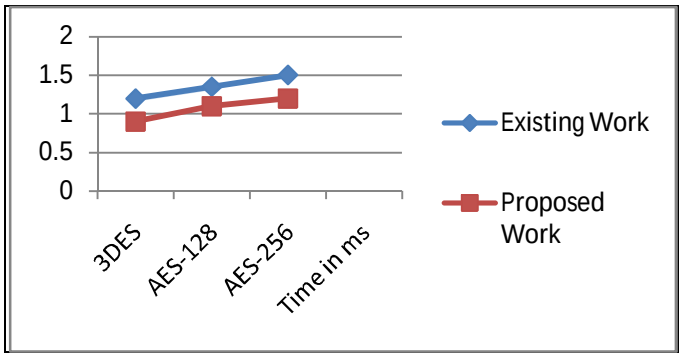


Fig 1.8: Average time taken by Decryption Algorithm (in ms)

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.

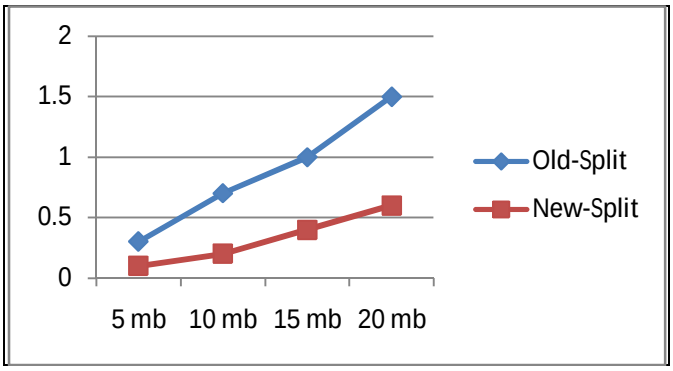


Fig 1.9 Average Time Comparison between Old Split and New Split Scheme.

In the above 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.

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

International Journal of Innovative Research in Computer and Communication Engineering
(A High Impact Factor, Monthly, Peer Reviewed Journal)
Website: www.ijircce.com
Vol. 6, Issue 12, December 2018

7.1 Comparison between Existing System and Proposed System

Comparison Factors	Existing System	Proposed System
Security Algorithms	In existing system, security algorithms AES-128 and AES-256 are used.	In our work, for high security we used File Splitting Concept which is more securing than AES-128, AES-256 and 3DES.
User's Private Key	Not used	Use for more secure file encryption.
One Time Password	Not Implemented	Implemented with 2 category i. OTP for Sensitive Data ii. MOTP for High Sensitive Data

Table 1.1: Comparison between Existing and Proposed System

VIII. CONCLUSION

Cloud Computing is the rising development and on account of the growing time it in like manner get broadening. As demonstrated when, the customers in the cloud is furthermore augments and with this genuine test is the security of the information set away in the cloud server. In our work we have inspected the security computations like TDES, AES-128/256 with the examination between them. Moreover we have exhibited new security framework in presence of File Split. By encounter each one of the results and diagrams of the proposed work, we can surmise that our work is a gainful and capable puzzle based system assembles execution of the cloud condition and besides lessens the taking care of time. Moreover concurring the need of the information, they get that kind of security. The framework shows that our proposed work give the better security when stood out from others.

As a part of the future work respective to our proposed work this can be overhauled with better security computations like Asymmetric figuring with better execution time, new systems and methods used for giving better security to the information, other way data gathering can moreover be used which enhance the structure. Moreover sensitive figuring systems can be used which give the customized data request and better methodologies for the mystery and uprightness of the information.

REFERENCES

[1] Yogendra Shah, Vinod Choyi, Andreas U. Schmidt and Lakshmi Subramanian, "Multi-Factor Authentication as a Service", 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 978-1-4799-8977-5/15 $31.00 © 2015 IEEE.
[2] A. Selcuk Uluagac_, Wenyi Liu, and Raheem Beyah, "A Multi-factor Re-confirmation Framework with User Privacy", 978-1-4799-5890-0/14/$31.00 ©2014 IEEE.
[3]. Mojtaba Alizadeh, Wan Haslina Hassan, Touraj Khodadadi, "Plausibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing", 2166-0662/14 $31.00 © 2014 IEEE.
[4]. Salman H. Khan and M. Ali Akbar, "Multi-Factor Authentication on Cloud", 978-1-4673-6795-0/15/$31.00 ©2015 IEEE.
[5]. Reza Fathi, Mohsen Amini Salehi, and Ernst L. Leiss, "Easy to use and Secure Architecture (UFSA) for Authentication of Cloud Services", 2159-6190 2015.
[6] A. Kundu, C. D. Banerjee, P. Saha, "Presenting New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 12, December 2018

[7] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Logical Cloud Computing: Early Definition and Experience," tenth IEEE Int. Meeting on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep.2008, ISBN: 978-0-7695-3352-0.
[8] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202. [9] 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, www.conference.thesai.org.
[10] Yibin Li , Keke Gai, , Longfei Qiu, Meikang Qiu , Hui Zhao, "Intelligent cryptography approach for secure distributed bigdata storage in cloud computing", Information Sciences 0 0 0 (2016) 1–13, www.elsevier.com/locate/ins, ©2016 Elsevier.
[11] Nelson Mimura Gonzalez, Marco Antônio Torrez Rojas, Marcos Vinícius Maciel da Silva, Fernando Redígolo, A system for confirmation and approval accreditations in cloud computing.12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[12] Tereza Cristina Melo de BritoCarvalho, Charles Christian Miers, Mats Näslundand Abu Shohel Ahmed, 2013. A system for confirmation and approval accreditations in distributed computing. twelfth IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.
[13] Mohammad Farhatullah, 2013. Snow capped mountain: An Authentication and Leak Prediction Model for Cloud Computing Privacy. third IEEE International Advance Computing Conference (IACC), 2013.
[14]. L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture," ICWS 2009: IEEE International Conference on Web Services, pp. 607-616. July 2009. DOI: 10.1109/ICWS.2009.144.
[15]. Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing," Draft Special Publication 800-144, 2011. http://csrc.nist.gov/productions/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.