INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Cloud based data storage by securing it through face recognition mode

Nadar Steffy Felicia Inbamani
steffyfelicia7@gmail.com
Rajalakshmi Engineering College, Chennai, Tamil Nadu

Kumar P.
hod.cse@rajalakshmi.edu.in
Rajalakshmi Engineering College, Chennai, Tamil Nadu

ABSTRACT

Trust of Clients cannot be completely trusted or beneficial through the cloud. Many information gets corrupted due to the unwanted users by the employees in the hierarchy of an Organization. Separate Organization handles the data securely, but in many cases, data is being given away for money because of the single level Management. We move forward to an advanced safe Technology to overcome this issue, where data are downloaded by an Organization or a set of admins in a hierarchy through face detection mode. If any of the admin rejects in accepting the request the file cannot be downloaded and thereby the data is made secure. Advanced Encryption Algorithm is the medium to make this technology secure and beneficial. Many such technologies can offer such a new form of security based work for efficient and brand form of storage process in the software as well as any other field in cloud computing.

Keywords— *AES, DES, CLOUD, SaaS, PaaS, IaaS*

1. INTRODUCTION

The formal description of Cloud computing in National Institute of Standard and Technology conveys that "cloud computing is a source which enables ubiquitous, convenient, network access being shared on the pool of resource computing configuration. The five main content which validates the entire functionality of the system.

- Provisioning the capabilities of cloud computing on demand self-services for storage as a server without the need for human interaction.
- The users can be resourced and can be undertaken, analyzed and made under control for giving a transparent for the two services namely the provider and the user. Automation control and Optimization of resource can be metered and leveraged for an appropriate form of servicing in cloud system [1].

1.1 Saas

Optimizing and providing any form of services for the level of the capacity in an appropriate type of servicing and a system must be automated and made under control for the most pronounced and functioned the efficient technology is the software as a service.

1.2 Paas

Executing the Programming language is many been provided by the service and has a platform namely Operating system, web server and for program validation, it uses the database.

1.3 Iaas

Encryption and Decryption is a form of technology used for security purpose in Cryptography, where the concept in detail is described as the form of converting the plain text into the cypher text with some coding or with any of the text form. Encryption is mainly done for security purpose.

It shows the detailed form of the system in which the system is all about securing user uploaded inputs from hackers by using face detection mode. It works efficiently in the same network of an environment. Here the system work is based on the hierarchy [2] of users (Admin). Once when the user uploads their inputs by using formal registration method of login, the file is encrypted in the database. Now, this information of the uploaded file is known to all the users in the hierarchy. If any one of the users needs to download the file, a request must be sent to all the users in the hierarchy for downloading the file and the port number will be notified in the request for face reorganization .if any one of the users in the hierarchy denies the request ,the file cannot be downloaded by the user who made a request .if all the users accept the request by face reorganization then the file can be downloaded .face detecting process is done by using mobile to system connection using if camera to assure that the user is from the same hierarchy.

2. LITERATURE SURVEY

Securing the data in any form of cloud storage is an efficient process and can be done in three modes as confidentiality, Integrity and Availability. Encryption and Decryption are the modes of the algorithm through which the system is able to do the functions efficiently. The private key is specified for Encryption in the symmetric algorithm and either of the way used for decryption. The public key is specified for encryption in the asymmetric algorithm and decryption made for public key in same form of the algorithm of securing data [3]. Cloud storage system has the mechanism for storage protection where

the two factors are to be described said by Joseph. The system gives an authority to send a message in an encrypted form and can be received back in a form which is also a cloud storage server. Sender's necessity is to receive his identity. Transparency of the sender is the most important form of cloud storage which won't be changed into decryption of either of the cypher text in any form of time [4]. Clustering is the method named as fuzzy and the main form of technology has the fuzzy algorithm for cloud computing in big data and produces a formation result in a heterogeneous cluster form and a small structure form is being designed in a dataset. To get this Problem to be corrected Optimization of the Objective form of sensor spaces makes an efficient technology in a higher order form [5].

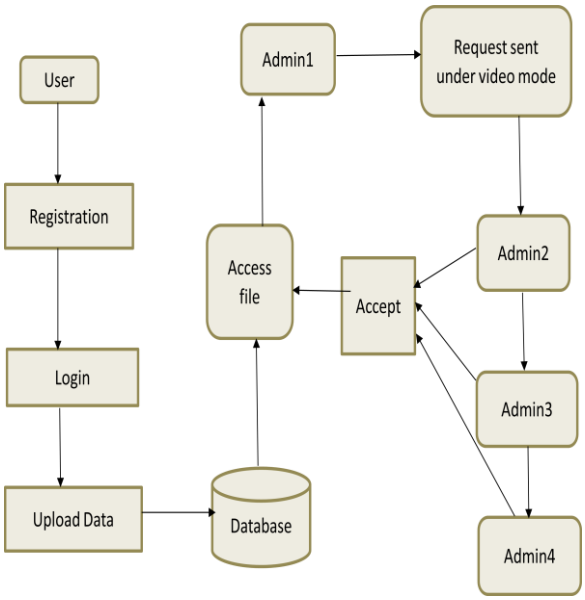
Single signing algorithm is an efficient technique for the development of any project based on its security in the form of any development in the field of security and the purposes of its work. The best solution is based on the trust and the working of any guaranteed privacy process of search data. An easy way of accessing any data can lead any kind of harm for the privately stored data in a particular field will make its trust among the users [6]. Security of any information is based on bytes and its process is an important form in cloud computing. Lots and lots of surveys are undertaken for the cloud storage security purpose in a high range of concern. Many views from various papers convey that cloud security has an aim to secure the information the raw data for the user efficiency and to increase the trust among the cloud environment. Security of a file is well structured in an efficient way of development that has efficiency in the cloud server and forms security in cloud storage [7].

Access of any information from the data storage using security, Integrity of data is most important in the verifying process in an outsourcing data for which the entire file can be downloaded and can be kept intact. Formal value of system and security model is viewed. Bilinear paring is modelled based on the identification of any such process in a concrete protocol. Efficiency in saving the cost of the one who verifies the cost in the protocol verification or can be said as checking is very important and efficient[8]. Level of big data analytics and its security in the cloud has a major cause in the application of any software process and its database. Cost of any computation can be decreased from the side of the user and verify its integrity for noticing the pubic verification process in any kind of environment. Server based on the audit can be used in case of the cloud server process for the file upload and for storing any form of data through which the entire cause can be followed in data integrity and verification process. Formation of any field in or any best form of application for the maintenance of any storage of data in the cloud makes the process effective and challenges the entire field of application for maintaining many huge burdens of computation in the devices of resource formation of any process [9].

Many analysis of how the data are made secure and functioned and processed in any form of level and its efficiency sector by maintaining the formation of security and the performance procedure in retrieval of any file from a document in the field of securing the data from unwanted user plays the most important role in the efficiency od cloud computing level of hierarchy. Attributes of encryption are also the form of securing information through broadcast, access control and for receiving a solution that gives its effectiveness [10].

3. PROPOSED STUDY

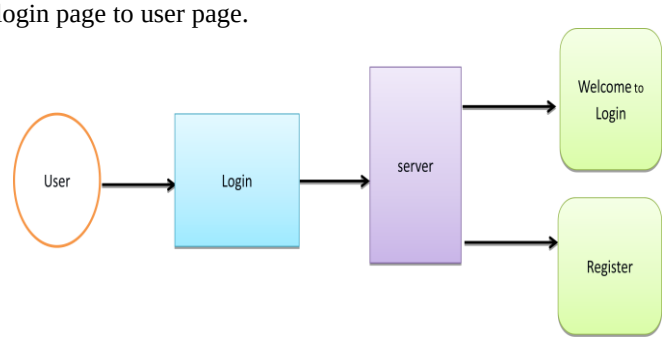
An efficient form of making the data secured is by having a new technology as per shown in the framework of the newly introduced system. The entire system is a framework of effective modules which refers to the functionality of the system working schemes. The framework initializes with the user and admin are two modules with the subdivisions in its working. The framework describes that the user has a sub module as registration, login, file upload and the centre medium is the database for the storage purpose. The database is the mediator to store the data from the user and admin can retrieve it based on its hierarchy. The gateway connects the database and the server. Initially, the user sends the data or uploads their information by registering and then by login with the specified password and thereby the file gets uploaded and it gets stored in the database where the information gets retrieved based on the request placed. Now the next main module where there are levels of admin i.e. Hierarchy of admin work together for the file to be downloaded which was once uploaded by the user. Here the uniqueness is that the user (admin or an Organization) can be found out based on the video mode. If any one of the admin requires the file of the user to be downloaded, the first admin should give request to all other admin in the hierarchy for downloading the file. If any one of the admin in the hierarchy denies by rejecting the request then the admin who requested for the data cannot download the file of the user. If all the admin accepts the request based on the face detection video mode then the data can be downloaded.



This system framework is one form of an architecture which comprises an effective way of data storage and a safe way of retrieving the file. The way of the methodology is to secure data through face recognition mode is the main reason behind how the entire system works and has an advanced encryption standard form of securing the information. The following modules are described with the following diagrams which give a clear view of how the system works.

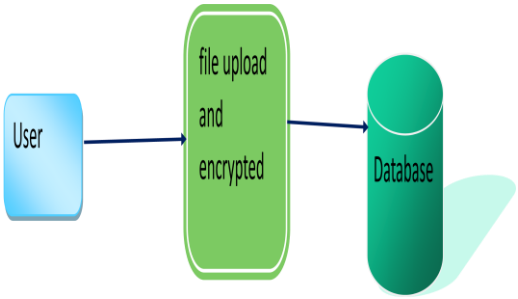
The first module is user interface which conveys the important role for the user is to move login window to user window. This module has created for the security purpose. Moreover, login page login id can be prevailed and processed and password can also be given as per users need. The procedure is to correct or validate the name id and password if it is validated or not for the betterment of the technique. If we enter an invalid username or password we can't enter into login window to user window it

will show an error message. We need the new and efficient form of saving the data from the unknown user moving into the login page to user page.

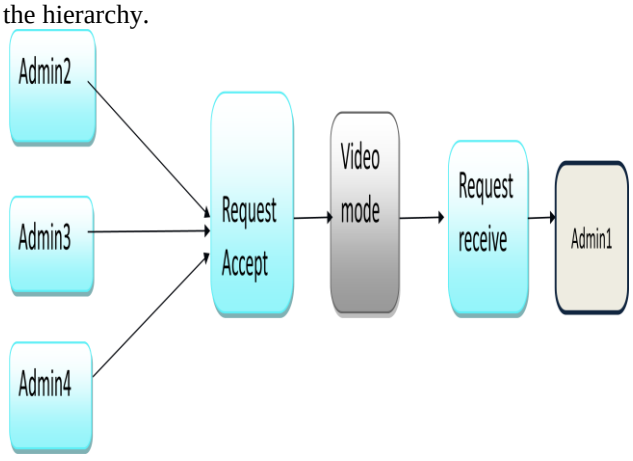


Here Advanced Encryption Standard is used as the encryption technique for securing the information.

The second module User will log in their account and upload a file or image, and that files/image are encrypted and stored in the admin side. Even uploaded user also doesn't access, before an admin can accept. The entire data for the user can be uploaded and processed for the entire function in storing the information. Any such informative process can be maintained in an effective form of appliances in the field of securing information.



Admin Monitoring File, in this part admin, will maintain the file, after that the admin will monitor the files in the way of video mode. If any one of the admin from the admin team is going to request a file, the request will go by video mode. Here admin has all the authority over the file they can access whenever needed but with the acceptation of all the user admin in the hierarchy.



4. EXPERIMENTAL RESULTS

The experimental result comprises of the Hardware, Software, Input and Output. This result formation is due to the process of making the evident use of the entire system and its working. It can be clearly viewed as a technique of securing all the information from the unwanted users as per the hierarchical form of acceptance of admin in the system.

4.1 Hardware requirements

The main hardware contents that the system is intact with is it has Dual core2 processor and contains 40 GB Random accessible memory, It comprises of 15" colour monitor and a 250 GB hard disk for the internal storage. The entire function and its efficiency of the results are supposed to be maintained and described as the hardware component.

4.2 Software requirements

The software requirement is an inner proportion of the effective working in a system its functionality is the front and back ends, its operating system. The Front end is J2EE (JSP servlets) Java Server Page, the Back end is MY SQL5.5 and its Operating system is the main working technology which has Windows 7, IDE is Eclipse. This is about the software requirements in the system for its efficiency and the level of formation for the growth of the entire system.

4.3 Input

The work to be carried is completely about the experimental operation based on coding for the entire system using an in web camera. Here in this phase it completely comprises based on the working of entire modules and it does the work of storing in a particular database, browsing, accept and reject process is carried out in the entire phase. The implementation makes to work the system with users and admin for Request and Response of the file. Implementation of mobile to system organization using ib web camera a mobile application in android which is a common and affordable tool and can be used by working people in an organization for securing information. The Proposed system works with the aim to achieve security of data. The input used here is the file upload and the request placed by the admin to all the admin in the hierarchy as a port number in the form of view notification process in the entire form of making the procedure an efficient system.

Fig. 1: Input

4.4 Output

The output is placed in the form of screenshots whereby the detail procedure can be explained and processed. Step y step process for the function to take place for the entire field of security. The second page is online data protection, here on this page it creates a medium for log in and to enter the password for moving towards the next level of page where the user can upload his/her data for securing with hope that it won't be hacked by any unwanted user thereby securing the information in a secured manner.

Many are the reasons under which many cases situation or the environment is changed and can be maintained for which all the process has to be functioned and maintained in the new form of maintenance.

And make sure of the requester.

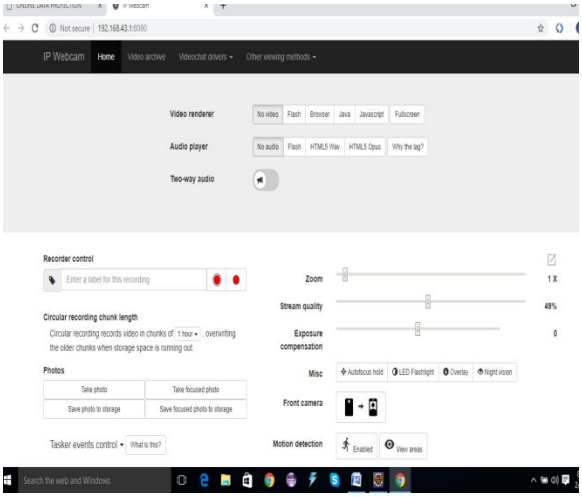


Fig. 2: output

After that, the requester can view as a download once when the other admin in the hierarchy is fine with the requester and accepts for downloading. If any one of the admin in the hierarchy declines then the admin1 cannot download the file and not even they can view the file they requested for. This is all about the system and its development for perfect security.

4. CONCLUSION

Encryption technique in Cloud computing has the most fatal part in securing data in a particular system and also has the tendency to manage any level of security for efficiency and best performance level in the entire system.

The new technology that is proposed has a particular standard of development in the new technology face detection process and has a vast process that is efficient in many of the organization with the biggest range of are under the valued area research. The simple and effective in the following developed approach is very efficient and proves for the better quality of security process in many fields, here Internet play the major role in the system for the purpose of browsing so as to reduce any kinds of complication in the system for its efficiency in its analysis. Through the face detection, it's made easy for the identification and has made a user-friendly environment for the user because nowadays biometrics also depends on the fingerprints which can give a strong hope for the user to upload their file without any means of interruption or simply can say from hacking.

In future, it can be used as the form of security through face detection or through sensors based on the entire globe of the same organization rather than a single zone and can have the efficiency in handling many levels of hierarchy to improve the performance and give strong hope among users based on security and maintenance.

5. REFERENCES

[1] Yang Yang, Xianghan Zheng, Chunming Rong, Wenzhong Guo (2017), 'Efficient Regular Language Search for Secure Cloud Storage', IEEE Trans on cloud computing, vol. 23, pp. 30-45

[2] Joseph K. Liu, Kaitai Liang, Willy Susilo (2016);'Two-Factor Data Security Protection Mechanism for Cloud Storage System', IEEE Trans on cloud computing, Vol. 23, pp. 30-45.

[3] Qingchen Zhang, Laurence T. Yang, Zhikui Chen, and Peng Li. (2017);'PPHOPCOM: Privacy-preserving High-order possibilistic c-means Algorithm for big data cloud computing', IEEE Trans on big data. Vol.25, pp.56

[4] Katai Liang, Xingi Huang, Funchun Guo (2016);'Privacy Preserving and Regular Language search over Encrypted cloud data', IEEE Trans on cloud security. Vol.36, pp.20-25

[5] Victor Chang, Muthu Ramachandran (2015),'Towards Achieving data security with cloud computing Adoption Framework', International Journal of Intelligent system and Application. Vol.08, pp.245-256.

[6] Atenise, R.Burns, R.Curtmola, L.Kissner (2014),'Identity based Distributed Provable data Possession in Multicloud Storage', International Journal of Computer Science and Electrical Engineering, Vol.1, No.2315-4209.

[7] Jin Li, Xiao Tan, Ducan S.Wong (2014), Enabling Proof of Retrievably in cloud computing with Resource-Constrained Devices 'IEEE Trans on Data Analytics, Vol.05, No.2.

[8] Deepnarayan Tiwari, G.R.Ganadharan (2015),' A novel Secure Cloud Storage Architecture combining Proof of Retrieval and Revocation', International Journal of Innovative Research in science, Vol.04

[9] S.M Lucas, T.J. Reynolds (2005),' Learning Deterministic Finite Automata with a smart state Labelling Evolutionary Algorithm', IEEE Trans on Complier Design., Vol.18, pp.45-49.

[10] B.Blaskovic, F.Skoplijanac-Macina (2018).'Discovering e-learning Process model from counter examples', International Journal of Computer Applications, Vol.92, No. 14.

[11] Dawn Xiading Song, D.Wagner, A. Perrig (2002),' Practical techniques for searchers on Encrypted data ', IEEE Trans on Software, Vol.09, No.2.

