IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

Securing cloud storage 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

In many cases benefits given by a cloud server isn't completely trusted by clients. Presently data are corrupted by the unauthenticated user with the help of employee's. Generally, data are securely handled by Separate Organization but some employees sell their access specifiers to hackers for money due to single level Management and data are not made safe. To overcome this issue we move towards Advance Safe technology where data are downloaded by the user (admin or organization) with the help of face detection video mode when they accept the user request by recognizing their face among the hierarchy of employees and then the data is shared from one place to another. Here Encryption Algorithm is used for sharing data in a secure means by detecting a face in the hierarchy.

Keywords— *Advanced Encryption Standard (AES), Data Encryption Standard (DES), Cloud hierarchy*

1. INTRODUCTION

The definition given by National Institute Of Standard and Technology (NIST) says that: "Cloud computing is a model for enabling Ubiquitous, convenient, On-demand network access to shared pool of configurable computing resources" [1]. The cloud is composed of five essential characteristics they are as follows:

(a) On-demand self-service: A user can provision computing capabilities, such as server time and storage, as needed without requiring human interaction.

(b) Measured Service-Cloud systems automatically control and optimize resource use by leveraging a metering capability appropriate to the type of service (example., storage, processing) .resource users can be monitored, controlled, and reported thereby providing transparency for both the provider and user of the service.

Cloud computing provides different services with these services are put into three models: Software as a service (Saas), Platform as a service (Paas), and Infrastructure as a service.

Software as a service (Saas): The services provided and optimize the resources by leveraging a metering capability appropriate to the type of services and the system has automatic control is transparent for provider and service. The more amount of security is being produced in the way it is created and monitored in the entire field of cloud computing.

Platform as a service (Paas): Computing platform such as web server, operating system and database and the background for programming language execution is provided by the service provider.

Infrastructure as a service (Iaas): Cryptographic is a technique followed by encryption and decryption. Encryption means the plaintext is converted into cipher text or some coded form of encrypting data through data security

2. LITERATURE SURVEY

Goals of securing the data are cloud storage includes three modes name confidentiality, integrity and availability. Two types of the algorithm are used in encryption symmetric and asymmetric algorithm. Asymmetric algorithm is used as private key encryption and is also used for decryption. They are also used as a public key for encryption and the private key is used for decryption [3]. Joseph describes the two-factor data security protection mechanism for cloud storage system the system allows the sender to send an encrypted message to a receiver through a cloud storage server. The identity of the receiver is the only need of the sender. The process is transparent to the sender. Most important in a cloud server cannot decrypt any ciphertext at any time [4]. Fuzzy clustering methodology is used as an important technique of c means algorithm for big data cloud computing for producing and efficient result in clustering formation for heterogeneous data and design for only small structured data set in order to overcome this problem the higher order form of big data clustering is done by optimizing the objective function in lesser space. The intention behind the development of any project is based on security in terms of a single signing algorithm is an efficient form [5]. Developing an approach towards security for an effective solution that must be trust or guarantee for the privacy of search data access of any data we can yield harm for the privacy of any user in any particular field will show its trust towards users. Real-time data security for bytes of data is important in cloud computing many surveys on security of cloud state the user security of data has the highest priority as well as concerned survey on cloud security states that the security of users can only be able to achieve with the Moto that is systematically adaptable of an efficient in cloud server in form of security [6]. Security of the store data for accessing information data integrity in form of remote checking is crucial important cloud storage checking for verification of an outsourced data is kept intact without downloading the whole data system model and security model or given formally a concrete which protocol is designed based on bilinear pairings checking protocol must be efficient to save the verifiers cost [7]. The methodology of big data analysis and the level of security in cloud computing is the application-oriented software process and database reducing the computational cost at user side during the integrity verification is the notion of a public verifiability process allowing the audit server on behalf of the cloud uses and preprocessing the data before according to the cloud storage server and later verifying the data integrity a new form of cloud storage formation in any field of appliances in the security and maintenance of the storage is the root form of cloud storage server the challenges and computational burden is to use for the users with resource devices[8]. The functionality of the analysis of how far the data security in any sector by maintaining the level of efficiency in the field of security of retrieval and performance. It uses their attributes based on encryption of broadcast access control to achieve an efficient solution. Finite automation from a set of label strings is the hard task that has been many studies within the machine learning community. Its performance is compared with the evidence of a state merging algorithm is equivalent to the learning of a regular language by the example of an application [9]. Efficiency regarding the level of a security in any information is done in methodology adopted learning is a system such as an intelligent tutoring system Deterministic Finite Automation (DFA) tutoring session is a run of the DFA or in process mining technology. Here we will process mining to discover and add new useful sessions for adaptive e-learning system [10].

3. PROPOSED STUDY

An efficient encryption technique for securing data using face recognition video mode rather than single signing algorithm. Here the data can be viewed or downloaded by any user who requests for a file, only when all the other users in the hierarchy accepts the request thereby securing the data from the hackers as the acceptation is done based on the face recognition mode. Even if a single user in the hierarchy rejects the request then the file cannot be viewed or downloaded by the requester and thereby the data can be secured [11]. A recent study about securing the information refers to protective privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is an essential aspect in any Organization of every size and type. One of the most commonly encountered methods of practising data security is the use of authentication. In authentication, the user must be provided with passwords which are now a day's easily hacked or some other form to verify identity before access to a system or data is granted. Data security technology measure is encryption, where data, software are encrypted and therefore rendered unreadable to unauthorized users and hackers. 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 works based on the hierarchy of users (Admin).Once when the user uploads their inputs by using formal registration method of login, the file is encrypted in the database [12]. 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 ib camera to assure that the user is from the same hierarchy.

4. CONCLUSION

Cloud computing is playing a major role in the system for securing data through encryption techniques and tends to be the major cause for securing the data in any level of management.

Using the Proposed method we improve the standard of securing data under the idea of face detection in many organizations and is an active research area with a wide range of application. The proposed approach is very simple and efficient in terms of securing data, even improves the quality of Authentication, It requires the only internet for browsing without any complicated analysis. Identification of person using face, it can be one of the most users friendly and frequently used in biometrics an easy process for face recognition. The major fact of any analysis in security concern will be hacking, thereby this proposed system will reduce the loss of security and will be an efficient process among users and gives a strong hope in their maintenance. Slight variation in acceptation will safeguard the data and the result will be efficient.

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 Retrievality 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 Compiler Design., Vol.18, pp.45-49.

[10] B. Blaskovic, F. Skoplijanac-Macina (2018).’Discovering e-learning Process model from counterexamples’, 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.