ACHIEVING DATA SECURITY WITH CLOUD STORAGE IN ADOPTION FRAMEWORK

Priyadharshini S[1], Sowmya M[2], Mrs Maheswari M[3]

[1, 2] *Student, Department of Computer Science & Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai, Tamil Nadu, India*

[3] *Assistant Professor, Department of Computer Science & Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai, Tamil Nadu, India*

ABSTRACT

Cloud computing provides flexible data management and ubiquitous data access. In existing system, an efficient large universe regular language searchable encryption scheme (data signing) is used. It has the tedious process work for decryption of files and data because tokens are need to be generated at the time of decryption. In proposed work, AES algorithm is used for uploading files. The files are encrypted initially and uploaded in the database. The data user sends the request to all admins and the admins verify whether the data user is authorized person or not using video mode. The proposed work reduces the time consumption compared to existing system.

.

Keyword : - *Encryption Techniques , Video mode Techniques*

---

1. INTRODUCTION:

Cloud storage is an emerging model of storage to provide scalable, elastic and pay-as-you-use service to cloud computing users. [1] A two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information. Cloud delivers convenience to the customers and at the same time arouses many security and privacy problems. Since the data are physically stored on the multiple servers of the cloud service provider, the customers cannot fully in charge of their data. [2] An important technique of fuzzy clustering in data mining and pattern recognition, the possibilistic c-means algorithm (PCM) has been widely used in image analysis and knowledge discovery. They worry about the privacy of the stored documents since the server may be intruded by hacker or the data could be misused by the internal staff for commercial purpose. [3] The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie- Hellman) problem. Over the last decade, privacy-preserving search over encrypted cloud data has been a meaningful and practical research topic for outsourced data security[4]. The customers prefer to adopt the encryption technology to protect the data confidentiality, which meanwhile arouses another problem: how to execute data retrieval on the large volume of ciphertext. [5] Cloud Computing Adoption Framework (CCAF) is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security, we use Business Process Modeling Notation (BPMN) to simulate how data is in use. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.

1.1 OBJECTIVE:

To address this issue, we investigate accomplishing catchphrase search over unique encoded cloud information with symmetric-key based check and propose a down to earth conspire in this paper. So as to help the productive check of dynamic information, we structure a novel Accumulative Authentication Tag in light of the symmetric-key cryptography to create a confirmation tag for each keyword. It has become a hot research subject in distributed computing security and various SSE plans have been proposed.

1.2 SCOPE OF THE PROJECT:

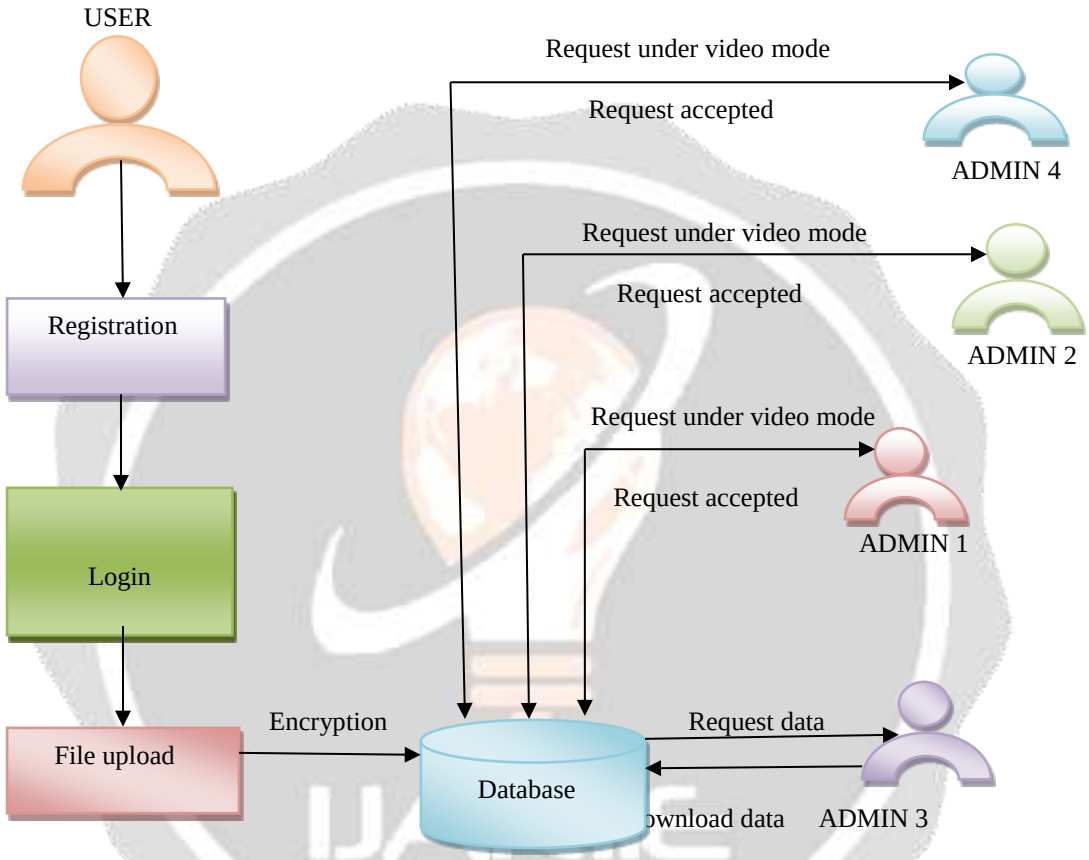
Present day society depends basically on compelling getting ready of the gigantic proportion of data assembled from a combination of sources. Diverse cloud-based organizations have been offered, including Microsoft Azure , Google Cloud, and Amazon EC2 , while various associations are needing to join this profitable market. The progressing improvement in the customers' solicitations has energized the plausibility of benefit sharing in cloud frameworks , where cloud owners can unexpectedly rent spare resources from one another to give better organizations to the customers.

2. RELATED WORK:

[1] A mechanism of two-factor data security protection is used with factor revocability for storage in cloud. System allows a sender to send an encrypted message to a receiver through a cloud storage server. A sender needs to knows only the identity of the receiver. The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. [2] An technique of fuzzy clustering in data mining and pattern recognition, the possibilistic c-means algorithm (PCM) used in image analysis and knowledge discovery. since it is initially designed for only small structured dataset. To tackle this problem, the paper proposes a high-order PCM algorithm (HOPCM) for big data clustering by optimizing the objective function in the tensor space. Further, we design a distributed HOPCM method based on MapReduce for very large amounts of heterogeneous data. Finally, we devise a privacy-preserving HOPCM algorithm (PPHOPCM) to protect the private data on cloud by applying the BGV encryption scheme to HOPCM. [3] Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification. [4] Using cloud-based storage service, users can remotely store their data to clouds but also the high quality data retrieval services, without the tedious and cumbersome local data storage and maintenance. Our security and performance analysis show that the proposed system is provably secure and more efficient than some searchable systems with high expressiveness. [5] Offering real-time data security for petabytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security using Business Process Modeling Notation (BPMN) to simulate how data is in use.

3. ARCHITECTURE DIAGRAM:

System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description language

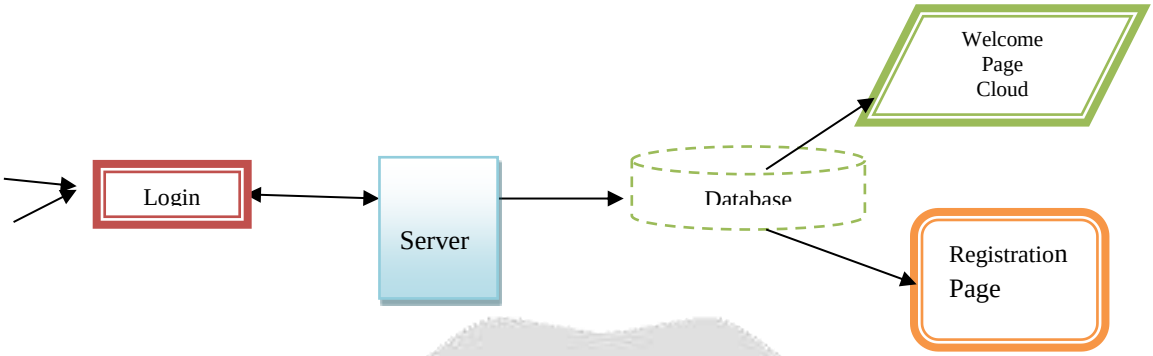


4. IMPLEMENTATION

4.1 FILE PROCESSING:

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the use. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using

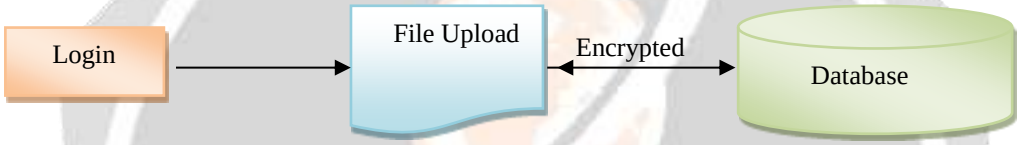
JSP for creating design. Here we validate the login user and server authentication.



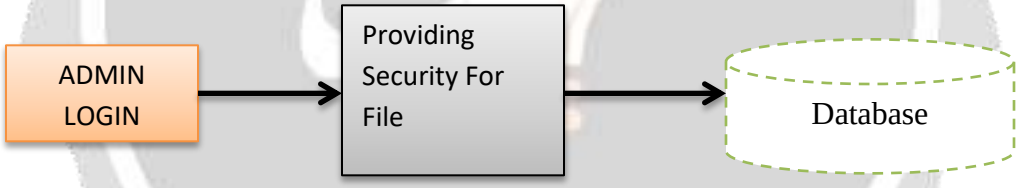
4.2 ENCRYPTION TECHNIQUE:

User will login their account and upload a file or image, and that files/image are encrypt and store in admin side. Even uploaded user also doesn't access, before admin can accept.

a) User login

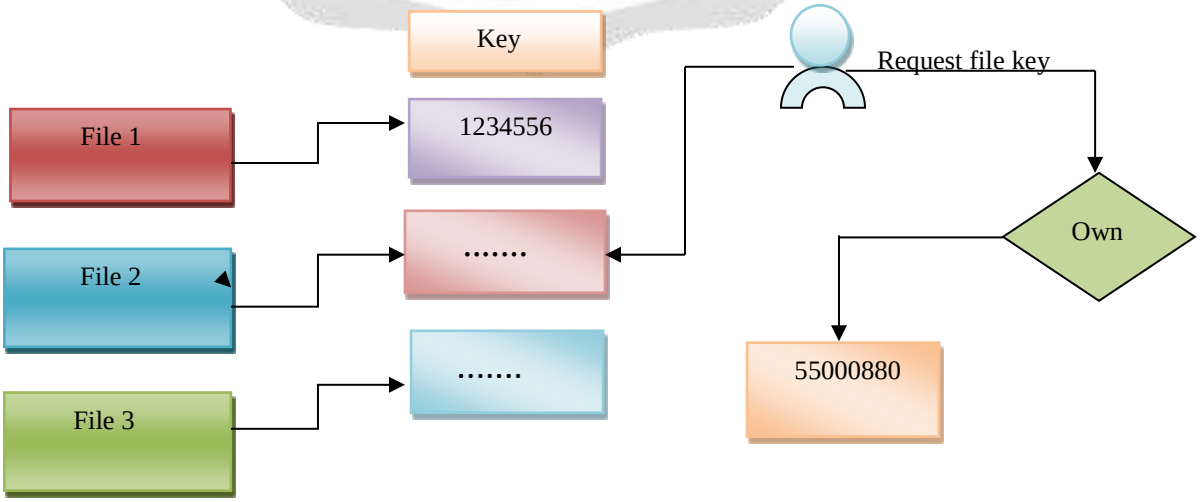


b) Admin login



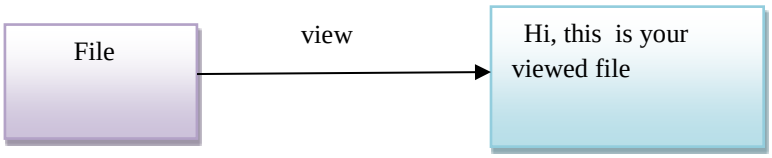
4.3 MONITORING:

In this part Admin will maintain the file, if the one admin from the admin team wants file they wants an acknowledgement of the other admins. The main motive is that secure the file.In this part admins will maintain the file, after that the admin will monitor the files in the way of video mode. If anyone of the admin from the admins team is going to request a file, the request will go by video mode.



4.4 FILE ACCESSING:

For reading each file which have been uploaded and split into 4 parts we should be owner of the file otherwise we should know the four different key which have been combined by random algorithm after reading the file you can also download the file otherwise with wrong key you can't open content.



5. CONCLUSION AND FUTURE ENHANCEMENT:

In this paper, we introduce a large universe searchable encryption scheme to protect the security of cloud storage system, which realizes regular language encryption and DFA search function. The cloud service provider could test whether the encrypted regular language in the encrypted cipher text is acceptable by the DFA embedded in the submitted search token. In the test procedure, no plaintext of the regular language or the DFA will be leaked to the cloud server. We also put forth a concrete construction with lightweight encryption and token generation algorithms. An example is given to show how the system works. The proposed scheme is privacy-preserving and indistinguishable against KGA, which are proved in standard model. The comparison and experiment result confirm the low transmission and computation overhead of the scheme.

For future work, an accumulation is often needed to gather the partial results from these parallel executions in different servers. The runtime system captures new events and run corresponding actions to analyze the page and store more URLs into the URL set to generate new events.

6. REFERENCES:

[1] Erl T, Cope R, Naserpour A. Cloud computing design patterns[M]. Prentice Hall Press, 2015.

[2] Li Z, Dai Y, Chen G, et al. Toward network-level efficiency for cloud storage services[M]//Content Distribution for Mobile Internet: A Cloud-based Approach. Springer Singapore, 2016: 167-196.

[3] Sookhak M, Gani A, KhanMK, et al. Dynamic remote data auditing for securing big data storage in cloud computing[J]. Information Sciences, 2017, 380: 101-116.

[4] Zhang Q, Yang L T, Chen Z, Li P. Privacy-preserving doubleprojection deep computation model with crowdsourcing on cloud for big data feature learning[J]. IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

[5] Zhang Q, Yang L T, Chen Z, Li P. PPHOPCM: Privacy-preserving High-order Possibilistic c-Means Algorithm for Big Data Clustering with Cloud Computing[J]. IEEE Transactions on Big Data, 2017, DOI: 10.1109/TBDATA.2017.2701816.

[6] Liu J K, Liang K, Susilo W, et al. Two-factor data security protection mechanism for cloud storage system[J]. IEEE Transactions on Computers, 2016, 65(6): 1992-2004.

[7] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[C]//Theory of Cryptography Conference. Springer Berlin Heidelberg, 2007: 535-554.

[8] Q. Zheng, S. Xu, and G. Ateniese. VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In INFOCOM, pp. 522C530.IEEE, 2014.

[9] Liang K, Huang X, Guo F, et al. Privacy-Preserving and Regular Language Search Over Encrypted Cloud Data[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(10): 2365-2376.

[10] Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework [J]. IEEE Transactions on Services Computing, 2016, 9(1): 138-151.

[11] Zheng X H, Chen N, Chen Z, et al. Mobile cloud based framework for remote-resident multimedia discovery and access[J]. Journal of Internet Technology, 2014, 15(6): 1043-1050.

[12] Chang V, Kuo Y H, Ramachandran M. Cloud computing adoption framework: A security framework for business clouds [J]. Future Generation Computer Systems, 2016, 57: 24-41.

[13] Barsoum A. Provable data possession in single cloud server: A survey, classification and comparative study[J]. International Journal of Computer Applications, 2015, 123(9).

[14] Wang H. Identity-based distributed provable data possession in multicloudstorage[J]. IEEE Transactions on Services Computing, 2015, 8(2): 328-340.

[15] J, Tan X, Chen X, et al. Opor: Enabling proof of retrievability in cloud computing with resource-constrained devices[J]. IEEE Transactions on cloud computing, 2015, 3(2): 195-205.