ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

Reckless Watchword Examination used for Translated Cloud Storing

[1] Priyanka.S, [2] Dr.KP.Kaliyamurthie
[2] Professor&Dean, Department Of Computer Science And Engineering, Bharath University
[1] Student , Department Of Computer Science And Engineering , Bharath University

Abstract: ***Cloud computing has generated a lot of interest within the analysis community in recent years for its several benefits, but hasalso raise security and privacy considerations. The storage and access of confidential documents are known united of the central problems within the space. Particularly, several researchers investigated solutions to go looking over encrypted documents keep on remote cloud servers. Whereas several schemes are planned to perform conjunctive keyword search, less attention has been noted on more specialized looking techniques. During this paper, we have a tendency to gift a phrase search technique supported Bloom filters that's considerably faster than existing solutions, with similar or higher storage and communication price. Our technique uses a series of n-gram filters to support the practicality.***

I. INTRODUCTION

As organizations and individuals adopt cloud technologies, many have become aware of the serious concerns regarding security and privacy of accessing personal and confidential information over the Internet. In particular, the recent and continuing data breaches highlight the need for more secure cloud storage systems. While it is generally agreed that encryption is necessary, cloud providers often perform the encryption and maintain the private keys instead of the data owners. That is, the cloud can read any data it desired, providing no privacy to its users. The storage of private keys and encrypted data by the cloud provider is also problematic in case of data breach. Hence, researchers have actively been exploring solutions for secure storage on private and public clouds where private keys remain in the hands of data owners. Boneh author proposed one of the earliest works on keyword searching. Their scheme uses public key encryption to allow keywords to be searchable without revealing data content. We have investigated the problem for searching over encrypted audit logs. Many of the early works focused on single keyword searches. Recently, researchers have proposed solutions on conjunctive keyword search, which involves multiple keywords Other interesting problems, such as the ranking of search results and searching with keywords that might contain errors termed fuzzy keyword search, have also been considered. The ability to search for phrases was also recently investigated. Some have examined the security of the proposed solutions and, where flaws were found, solutions were proposed. We present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus.

II. RECKLESS WATCHWORD EXAMINATION

A phrase search scheme that achieved further reduction in storage cost. The technique exploits the space-efficiency of Bloom filters to perform conjunctive keyword search and phrase search. Similar to other techniques, a set of keyword to document Bloom filters and a set of keyword location filters are used. The former enables the verification of existence of keywords in individual documents, by simply adding the keywords as members, and the latter allow the identification of keyword locations, by concatenating keywords to their locations prior to adding them as members. The conceptually simple scheme achieves the lowest storage cost among existing solutions.

III. RELATED WORK

There exists a specific security issue in symmetric searchable encryption that, when doing CKS (Conjunctive Keywords Search), the trapdoors and search results may reveal the relationships between the keywords being searched. For example, if the search result of keywords set A is the superset of keywords set B's, it indicates A is a subset of B by a high chance. Most existing search methods that support CKS suffer from such inclusion-relation (IR) attacks. We define measurements on IR security and propose CKS-SE, a secure CKS scheme based on bloom filter that achieves IR-secure by randomizing and integrating expressions of

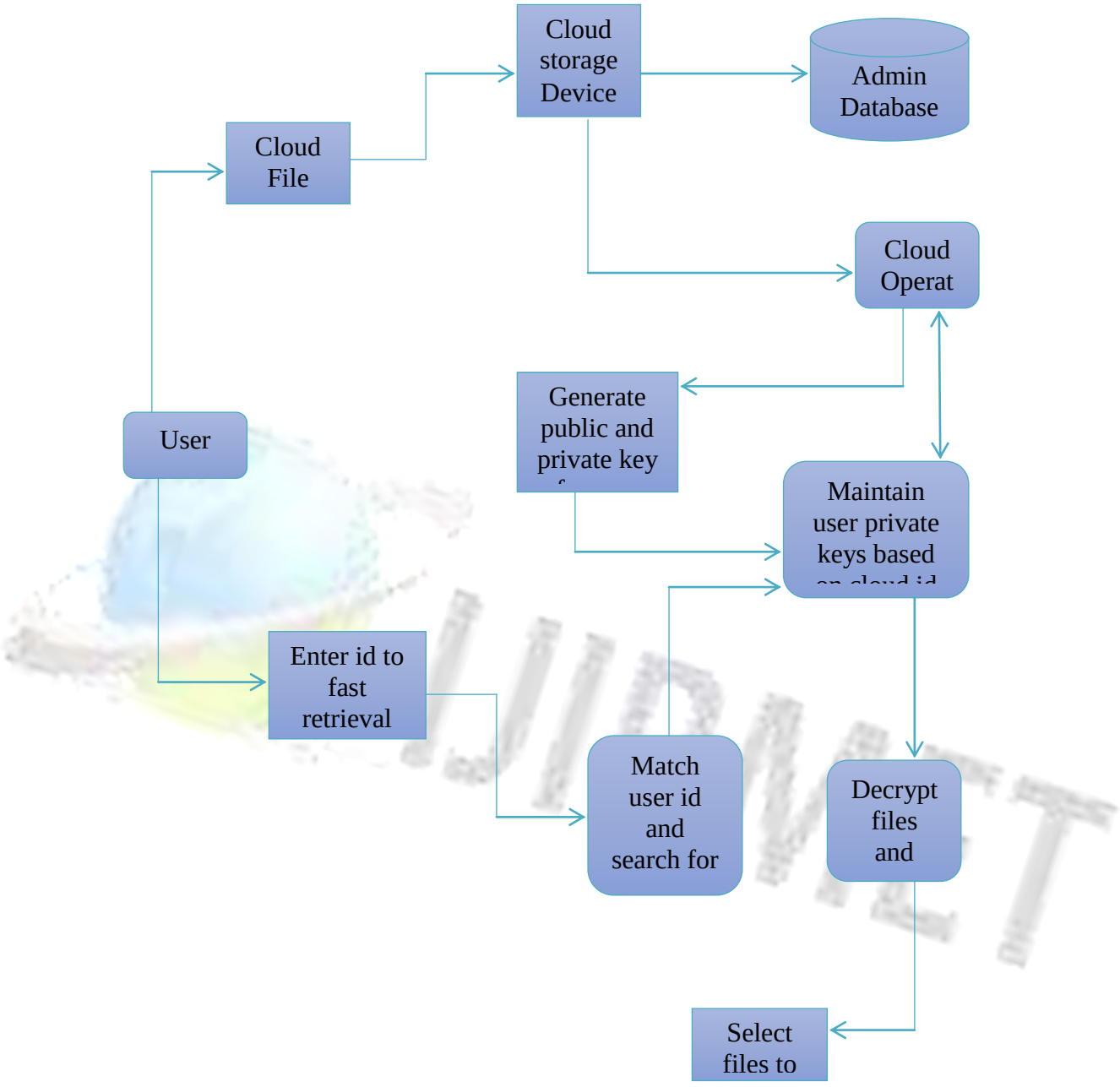
trapdoors. Experiments show that the average false positives are within an acceptable rate, and the performance of CKS-SE is among the best ones. As cloud computing is increasing in popularity, it is difficult to both maintain privacy in datasets while still providing adequate retrieval and searching procedures. This Paper introduces a novel approach in the field of encrypted searching that allows both encrypted phrase searches and proximity ranked multi-keyword searches to encrypted datasets on untrusted cloud. By storing encrypted keyword-location data along with specially truncated encrypted keyword indexes in a relational database, we are able to allow for a full range of search features in our encrypted searches, something that has never been accomplished before. Furthermore, our approach permits the encrypted corpus and index to both be stored on cloud data servers.

IV. EXISTING TECHNIQUE

The challenge for data privacy also arises as more and more sensitive data are being outsourced by users to cloud. Encryption mechanisms have usually been utilized to protect the confidentiality before outsourcing data into cloud. Most commercial storage service provider is reluctant to apply encryption over the data because it makes deduplication impossible. The reason is that the traditional encryption mechanisms, including public key encryption and symmetric key encryption, require different users to encrypt their data with their own keys.The first problem is integrity auditing Cloud server relieves users from additional burdens of storage maintenance and management. The other problem is security in deduplication. Rapidly adapting cloud services are in side to high volumes of data stored in remote servers of the cloud.

V. PROPOSED SYSTEM

A phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost. Our technique uses series of n-gram filters to support the functionality. The scheme exhibits a trade-off between storage and false positive rate, and is adaptable to defend against inclusion relation attacks. A design approach based on an application's target false positive rate is also described.



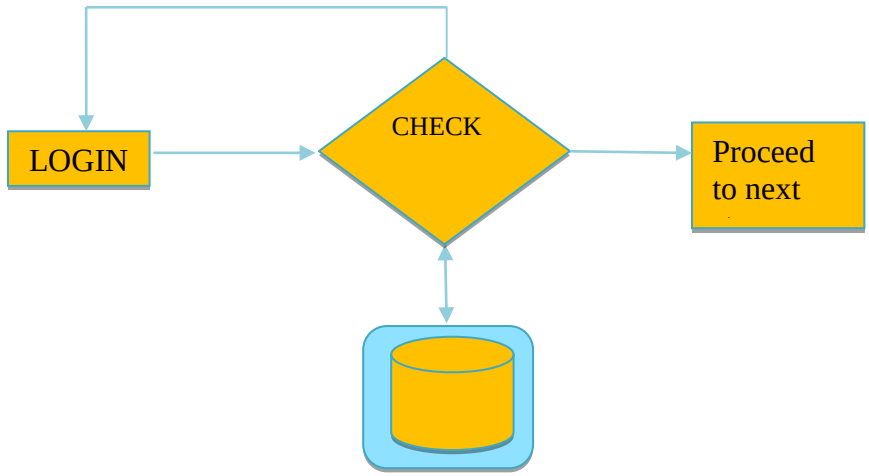
VI. MODULE DESCRIPTION

MODULE USER

Authentication:

The Sender need to enter exact username and password. if login success means it will take up to main page else it will remain in the login page itself.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

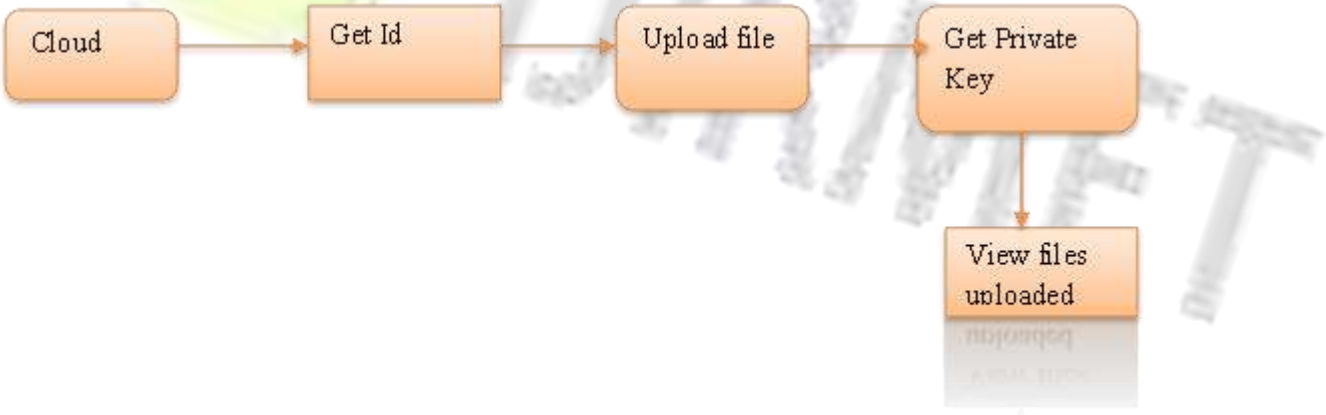


Upload file to cloud

In this module the authorized person store data into cloud that the data will be access the registration user only.

CLOUD ACCESS

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.



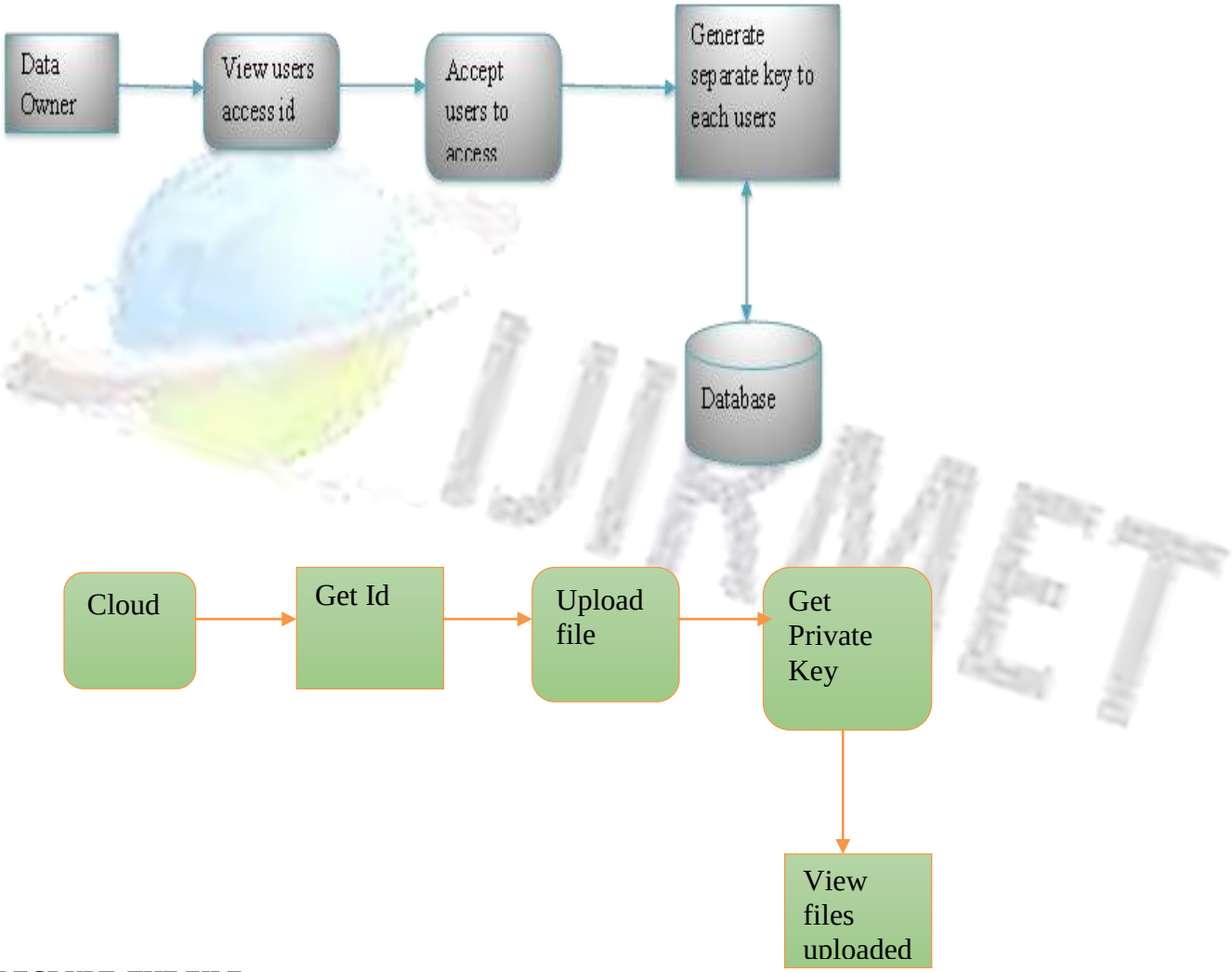
CLOUD ACCESS

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

ACCESSING CLOUD USERS FROM DATA OWNER

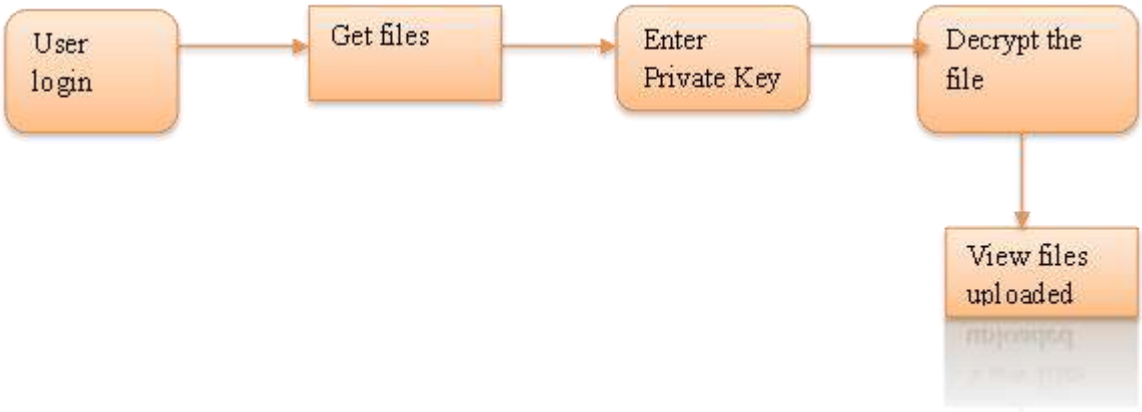
The process of identifying an individual usually based on a username and password. In security systems, Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. In authentication module is used to security purpose. Here this module only for user, after registration user enter the username and password. This input is check into the database, whether input is correct or not. If input is correct then allow to next process otherwise consider as a non-authenticated user.



DECRYPT THE FILE

In this module the authorized person store data into cloud that the data will be access the registration user only.Then User to Decrypt the file with Key .

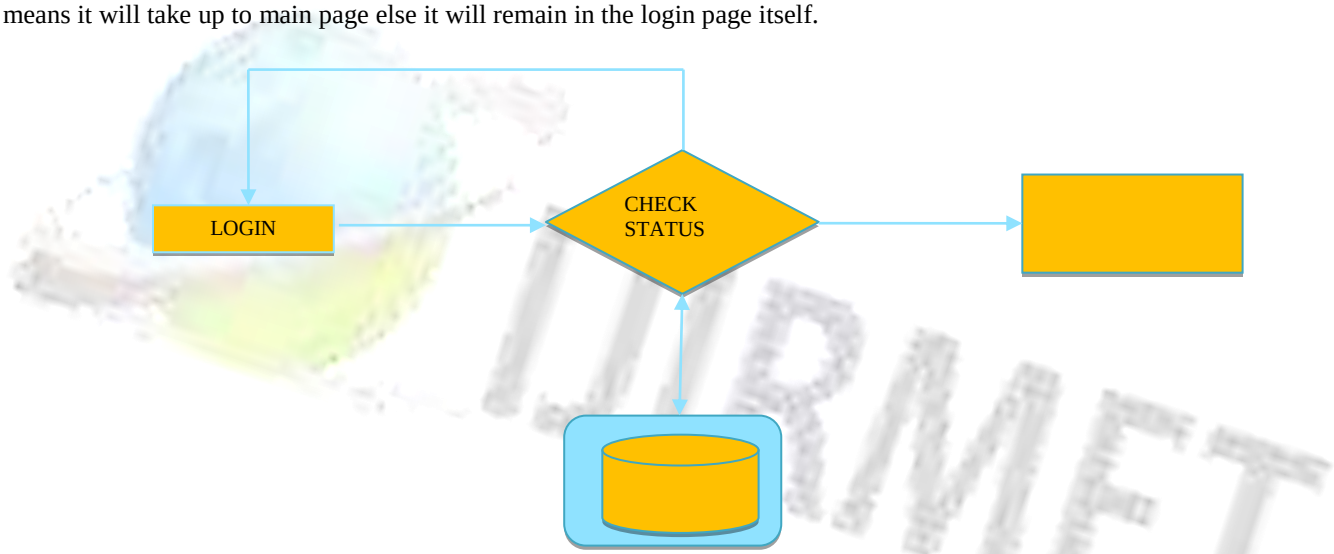
ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018



ADMIN

Authentication:

Admin has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

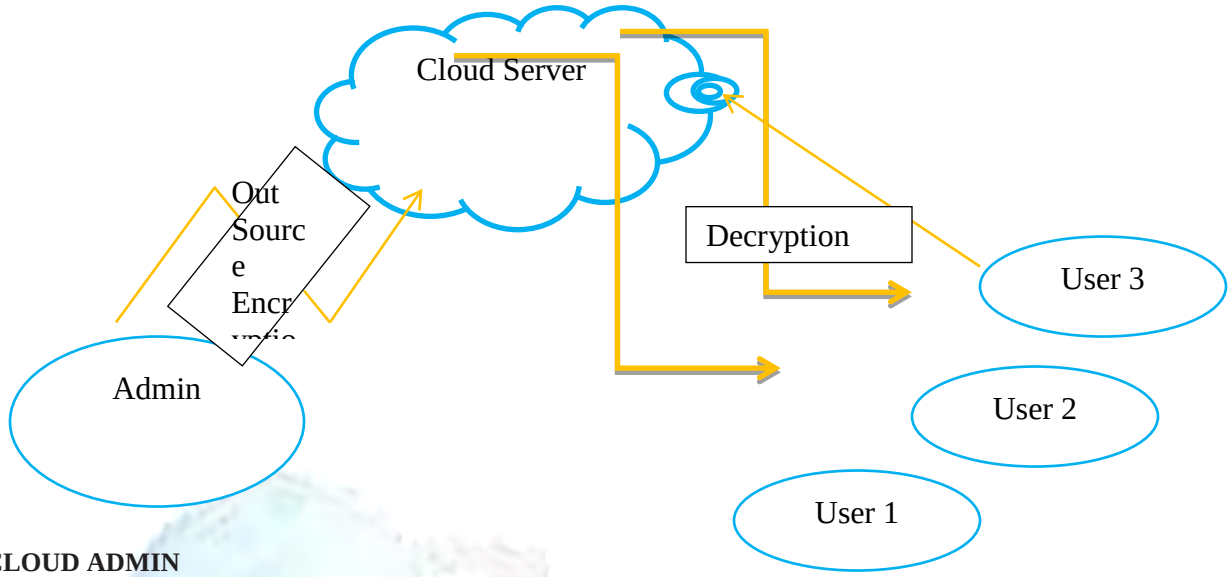


View the Files

In this module, Admin can view the File Details. If admin can view the File status, admin can also delete particular Data's or Details.

Cloud Storage

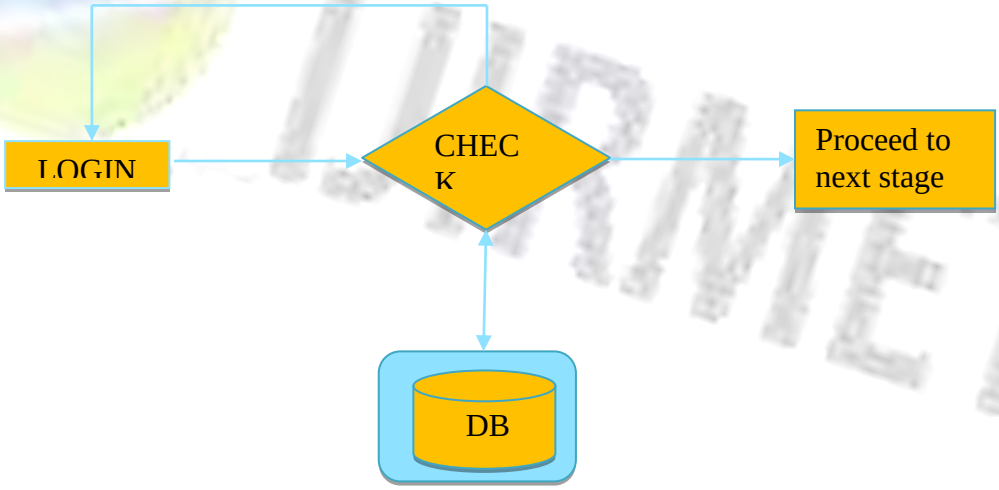
ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018



CLOUD ADMIN

Authentication

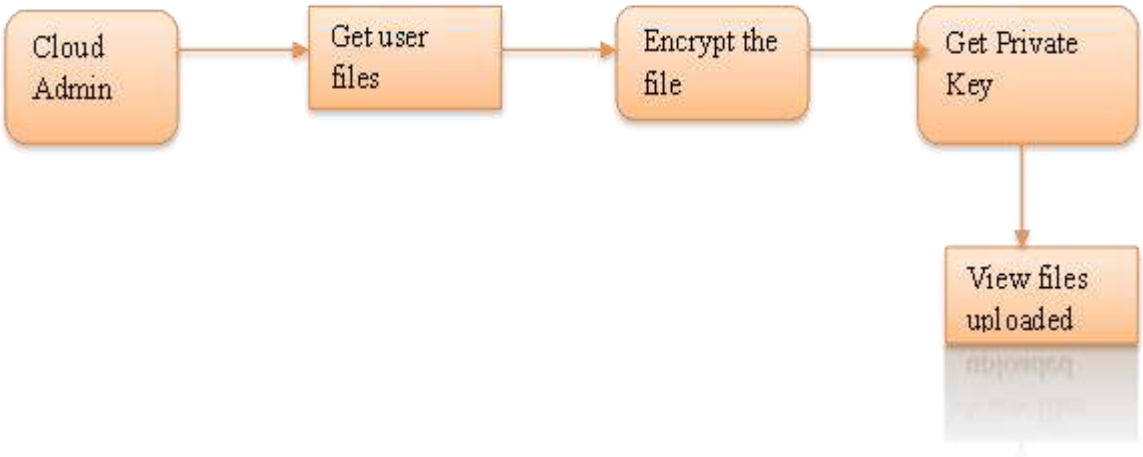
Admin has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.



ENCRYPT THE FILE

In this module the authorized person store data into cloud that the data will be access the registration user only. Then cloud admin to encrypt the user file with key Generation.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018



VII. CONCLUSION

our schemes do not require sequential verification, is parallelizable and has a practical storage requirement. According to our experiment, it also achievesa lower storage cost than all existing solutions except,where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application. An approach is also described to adapt the scheme to defend against inclusion-relation attacks. Various issues on security and efficiency, such as the effect of long phrases and precision rate, were also discussed to support our design choices
.

VIII. FUTURE ENHANCEMENT

To address the issues, much efforts have been made towards development of an encrypted cloud system One of the key features being investigated is the ability to search over encrypted data Although many have proposed solutions for conjunctive keyword search, few have considered phrase searching techniques over encrypted data. Due to the increased amount of information required to identify phrases, existing phrase search algorithms require significantly more storage than conjunctive keyword search schemes.

REFERENCES

[1] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Publickey encryption with keyword search,” in In proceedings of Eurocrypt, 2004, pp. 506–522.
[2] B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in Network and Distributed System Security Symposium, 2004.
[3] M. Ding, F. Gao, Z. Jin, and H. Zhang, “An efficient public key encryption with conjunctive keyword search scheme based on pairings,” in IEEE International Conference onNetwork Infrastructure and Digital Content, 2012, pp. 526–530.
[4] F. Kerschbaum, “Secure conjunctive keyword searches for unstructured text,” in International Conference on Network and System Security, 2011, pp. 285–289.
[5] C. Hu and P. Liu, “Public key encryption with ranked multikeywordsearch,” in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109–113.
[6] Z. Fu, X. Sun, N. Linge, and L. Zhou, “Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query,” IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.
[7] C. L. A. Clarke, G. V. Cormack, and E. A. Tudhope, “Relevance ranking for one to three term queries,” Information Processing and Management: an International Journal, vol. 36, no. 2, pp. 291–311, Jan. 2000.