# DESIGNING AN EFFICIENT CLOUD STORAGE TO PROTECT THE DATA FROM OFFLINE KEYWORD GUESSING ATTACK

B. ARUNMOZHI, Assistant Professor,
Department of Computer Science and Engineering

AJISHA R. J, Student of Computer Science and Engineering
St. Joseph College of Engineering, Sriperumbudur, Chennai.

SANJANA , Student of Computer Science and Engineering
St. Joseph College of Engineering, Sriperumbudur, Chennai.

## Abstract:

Cloud computing gives adaptable information, the executives and universal information access. Nonetheless, the capacity administration gave by cloud workers is not completely trusted by the clients. Accessible encryption could all the while give the elements of classification assurance and protection safe guarding information recovery, which is a crucial device for secure capacity.

Hence we propose an “efficient large universal regular language searchable encryption” scheme for the cloud, which protection is saving and securing against the off-line” keyword guessing attack” (KGA). A striking features of the proposition over other existing plans is that it underpins the customers language encryption and “deterministic finite automata” (DFA) based information recovery.

The huge development of the universe guarantees the extendibility of the framework, where in the image set should not be predefined. Various clients are upheld in the framework, and the client could create a DFA token utilizing his own private key without communicating with the key age place. Besides, the solid plan is effective and officially demonstrated secure in standard model. Broad correlation and the re-enactment shows that this plan has worked and executing predominant than different plans.

**Key Terms**: HTML-Hypertext mark-up language, JAVA, JSP-Java server pages, Java Script, My SQL-Structured query language, JDBC-Java Database Connectivity.

## Introduction:

The main aspect is to give a general insight into the analysis, description and requirements of the existing system that is facing the trust challenge, legitimate and serious concerns about privacy of such data. To mitigate these or situation for determining the operation of its characteristics of this document plays a vital role in the web development life cycle (SDLC) as it describes the complete requirement of the system in the situation. It is meant for use by the developers and will be the basic during the testing phase. Any change made to the requirement in the future will have to go through formal change as staged method approval process as one important function that is most required in developing this system which means the SRS and solving all the requirement that is important for the development of the system.

Demonstrating the system and installing the system at the client's location after the acceptance testing is successful. Submitting those required user manual describing the system interfaces to work on it and also the documents of the system conducting any user training that might be needed for using the system maintaining the system for the period of one year after installation that they tend to have with in the upcoming evaluation the of the resources available for the installation.

## Objectives:

- The in hand searchable encryption schemes only support and uphold some basic and general search methods in use , like the single keyword search, conjunctive keyword search and Boolean search. Thus the cloud computing is an ever evolving and fierce competition industry, it is of peek importance to exhibit good user experience. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.

## Literature Survey:

This paper "Privacy preserving similarity search with efficient updates in distributed key value stores" is proposed by wanyu Lin, member ., IEEE, Helei cui , Boachun Li., fellow , IEEE And Cong Wang have established the work on SSE .

Data should be outsourced in order to make the implementation of array performance with prototype on Microsoft azure and conduct an evacuation using a real world dataset. Reference taken from V.Vo, S.Lai, X.Yuan, S-F Sun, S.Nepal and J.K Liu on the description of internet conference applying cryptography network security which was published in 2020 limitations is high Chances of bottle neck and SGX enclave on the title accelerating forward and backward private searchable encryption using trusted execution.

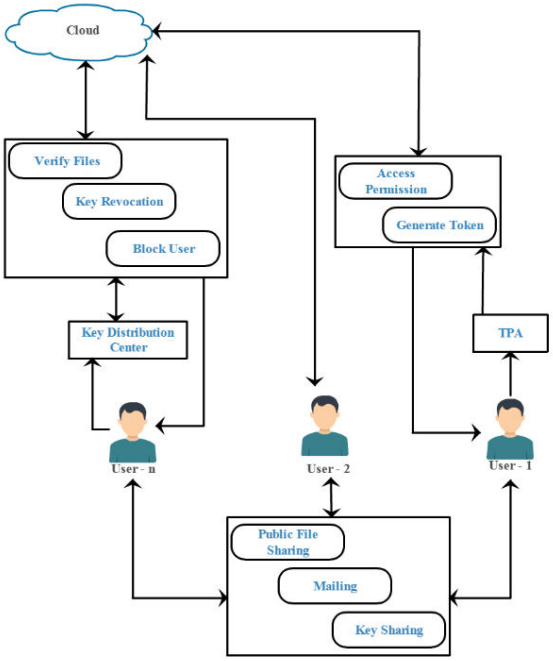
Another reference is of the title dynamic searchable in very large data base data structure and implementation its author is D.Cash et al.., of description network distribution system secure symbolic model proven symmetric at the year 2019 with the limitation of poor performance of efficient dictionary when stored on disk.

## System Design:

The proposed system outstands the drawbacks issued by the existing system thus we are proposing a striking novel, simple and efficient method to increase the protection of the data from the off-line keyword guessing attack.

An efficient large universal regular language searchable encryption scheme for the cloud which is privacy preserving and secure against the multiple possible attack. A notable highlight of the proposal over the other existing scheme is that it supports the regular language encryption and DFA that includes in it. Other existing scheme is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. Large universal construction ensures the extendibility of the system in which the symbol set does not to be predefined multiple users are supported in the system and the user could generate a DFA token using own privacy key without interaction with the key generation place.

The proposed project are beneficial only if they can be turned into information system that will meet the organizations operation requirement simply sated this test of feasibility asks if the system will work when it is installed.

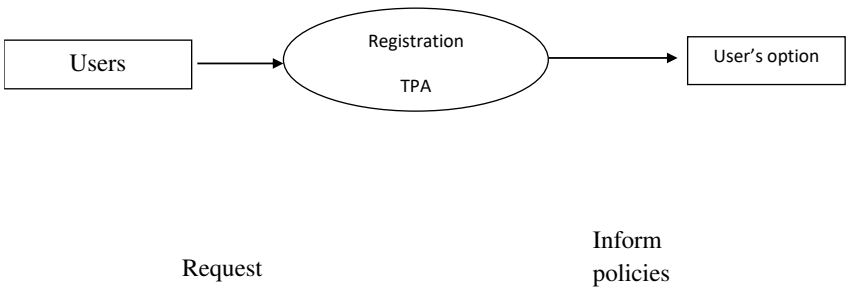



.

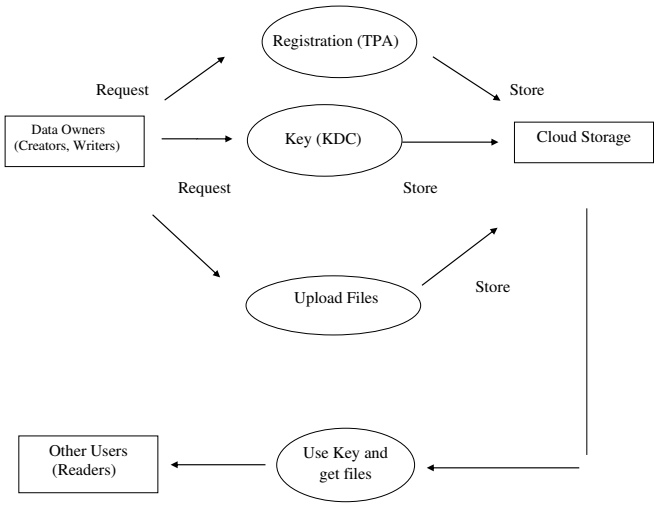
The archietecture deals with two to many users namely user 1 to user n, at the first the users will be sharing his profile ,mailing and key sharing process takes place in the 1st modulo then the user will be verified in the third party authority with the process of authentication involving the access permission , generate token with the private key that he have in access without the permission or information to the key generate place and all this methodology will be stored in the cloud and again accessible in order to have the verification process in due All the users have different need and objective that will help us to classify the verification process as you can see in the above diagram the one who is in the need to access files or just have to share their resources wants to send the request to the TPA for registration then the client makes the request to the key manager for the public key which will shared according to the policies there will be different policies for different public keys so that the client will generate the combination of user name and password as security credentials then the file is encrypted with public key and private key and transferred to the cloud

The TPA provides the rules and regulations that should be followed by the creators, users, readers.

The can get hold of the information they are looking for by clearing the authentication process.



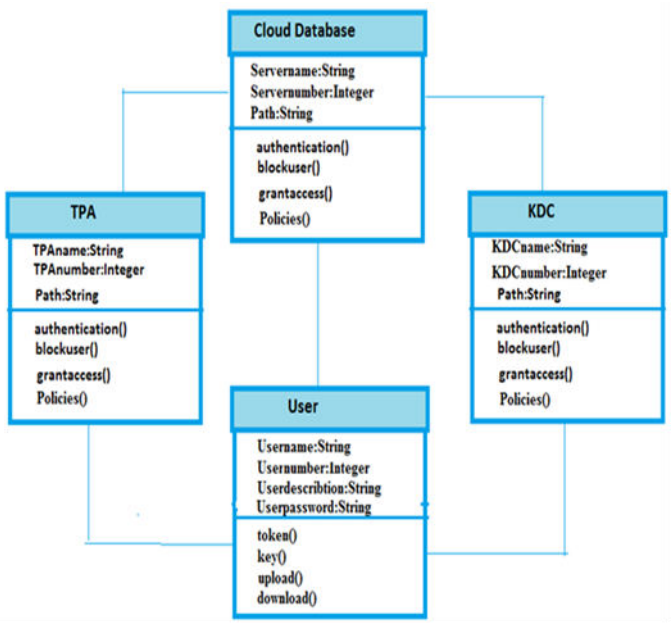
As the public is under the protection of the key manager the client should request for the public key to the manager thus the authenticated client gets the public key then the client can decrypt with the public and the private key. The credentials of the users where stored in the cloud only also while downloading the file the user will be authenticated once again for the verification cause the security of the information is top priority though the cloud don't any details about the client at all . File creator after getting proper authentication uploads his files in the clouds. The policy of a file may be revoked under the request by the clients, when expiring the time period of the contract or completely move the files from one cloud to another cloud environment. In the situation if any of the one statement is truly existing the policy will be triggered and the key manager will completely removes the public key in association with its file so that
no one can say that the file is assuredly deleted.




Key Distribution place which are decentralized generate different keys to different types of user after getting authorized token from users. To re-intake the file, the client must request the key manager to generate the public key. For that the client must be authenticated. Ability to limit and control the access to host systems and applications is via communication links . To achieve, access must be identified or authorized. After achieving the authorization process the client must associate with correct policies with the files. can neither use or re-enter the cloud circumference.

## Implementation:

The major inputs required in that for the web based accommodation can be categorized module-wise. Typically all the information is managed by the software and in order to get a access to those information one has to be authorized by entering one's username and password ever owner has their own domin to interact, in which the access is dynamically refrained rather denied. The result we gain from it will be are the system tables and reports, tables are developed dynamically to cover up the requirements on demand the usual gist of the entire information that carries across the institution. This application will be able to result output for the different input of the modules according to the situation.




The above is the tabular classification that is going to classification criteria for the modules. Thus it contains cloud database as for a table, kdc information like kdc-name and kdc-number to the clients then we have the user table which contains the general information of the users these are the important tables at use.

In general the user requests the key to the kdc who checks for the authentication with the TPA where the use must be registers in order to hold the access of the public key he is requested to the kdc , with that respected public key and the policies the user creates the user name and password with credential sources to have the access of the information in the cloud storage documents.

AES (acronym of Advanced Encryption Standard) is a symmetric encryption Algorithm. The algorithm was developed by two Belgian cryptographer Joan Deamen and Vincent rijmen.

AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192 and 256 bits

**STEPS IN ADVANCED ENCRYPTION STANDARD:**

**STEP 1**

Derive the set of round keys from the cipher key

**STEP 2**

Initialize the state array with the block data

**STEP 3**

Add the initial round key to the starting state array

**STEP 4**

Perform nine rounds of state manipulation

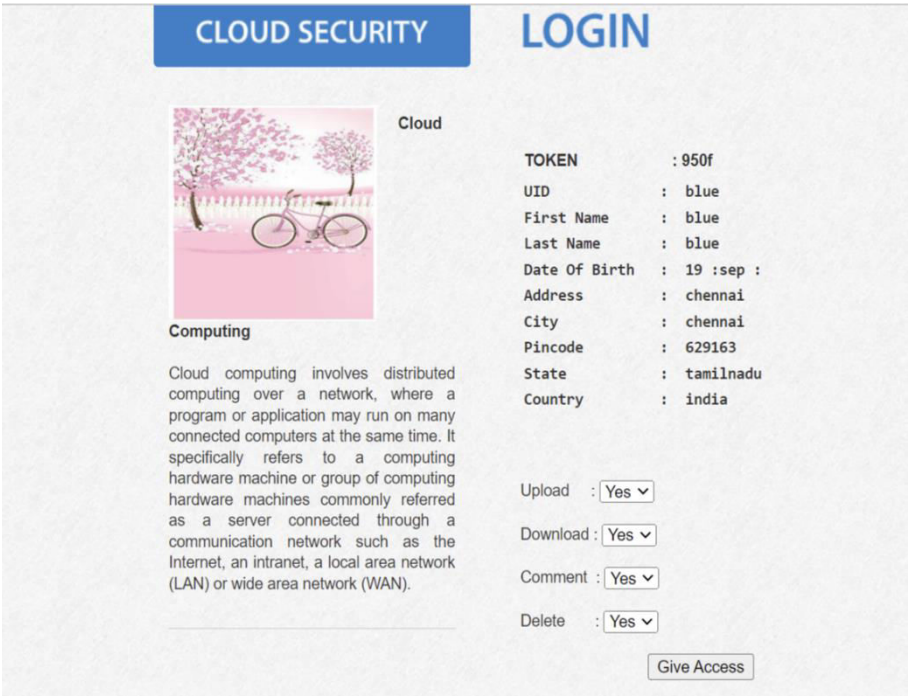
**STEP 5**

Perform the tenth and final round of state manipulation

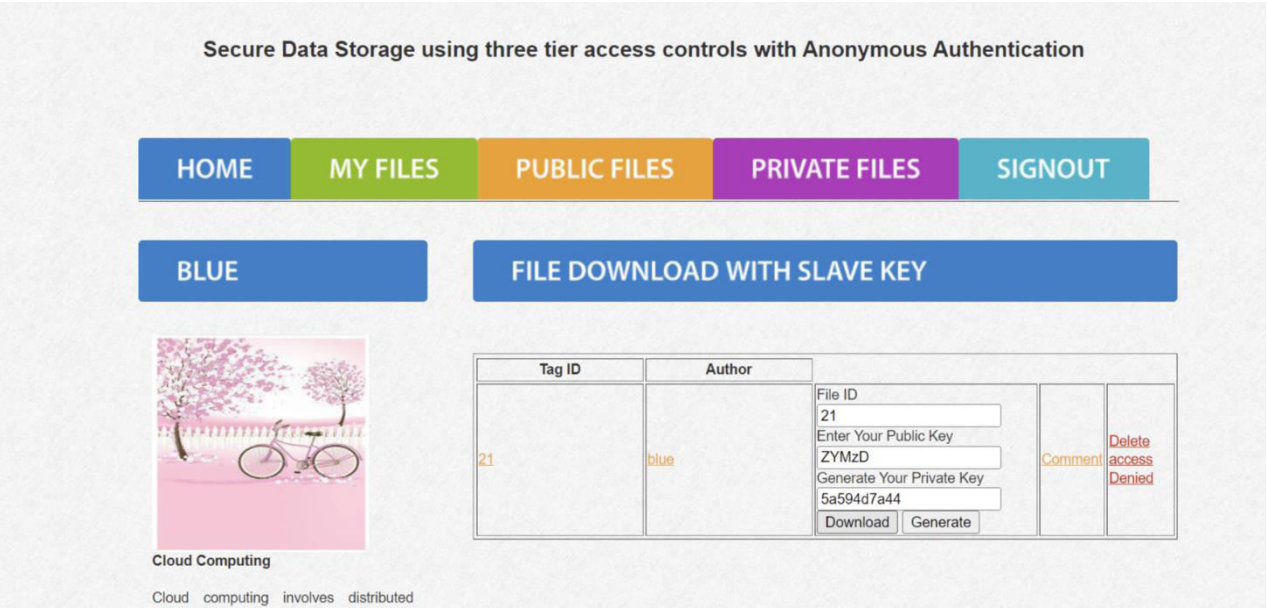
**STEP 6**

Copy the final state array out as the encrypted data

**Cloud security page displaying the login details and the specification of the clients/user involved in the process**




**Secure data storage using three tier access controls with anonymous authentication id displaying along with the tag id and author name**




## Conclusion:

Placing the focus on the catchphrase search over encoded information , it results a semantic based component watchword sear (scks) conspire. To carefully separate the semantic data of watchwords, we initially introduce an philosophy based compound creative idea, semantic comparability figuring technique (CCSS), which helps significantly to develop the precision

of closeness estimation between compound ideas by thinking about the compound great features that involves what's more, an huge amount of data sources in metaphysics. At those point, the SCKS plan is improved with the help of coordinating CCSS with LSH and SKNN. Not being able to face a semantic-based watchword search, SCKS can achieve multi-watchword search and positioned watchword search at the same time. Since both documentation is filed solely, the step up of one archive will never influence the other archives, which indicates that SCKS can bolster dynamic information fecundly. To update the security of SCKS, we propose a security-upgraded SCKS (SE-SCKS) by introducing a pseudo-irregular capacity. Alert security investigation of each SCKS and SE-SCKS is provided, and the examination on decent world dataset show that the introduced methodologies present is less overhead on conclusion and that the inquiry on time, beats the current plans.

## Future Enhancement:

- In Local Committee Network, the introduced inter mixed encryption mechanism may be altered for transmitting the sensitive data from work station to host based applications.
- In web based applications, the introduced mechanism makes the transaction of sensitive data from one user to another user, from any user to the server and from one server to any other server which are placed outside of the institution.
- In a cloud circumference, many numbers of people are in the hold of the web server locally or globally to exchange the sensitive data. The proposed inter mixed encryption technique is very helpful to improve the security and safety for web based transactions in future.

## Biography:

Mr.B.Arunmozhi M.E., is an Assistant Professor in the Department of Computer Science and Engineering at St.Joseph College of Engineering,Sriperumbudur, Chennai, Tamil Nadu. He has completed his M.E, CSE under Anna University Affiliation College in the year 2011. He has done his B.E,CSE under Anna University Affiliation College in the year 2007. Mr.B.Arunmozhi has 11 years of teaching experience and has 12 publications in International Journals and Conferences. His area of interests includes Network Security, Computer Networks, Data Science and Machine Learning. He is an active member of CSI and IEANG. He has organized various International Conferences, workshops and Seminars in the area of Computer Networks Computing & amp; Machine Learning respectively.

Ms.Ajisha R.J B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering, Sriperumbudur, Chennai, TamilNadu.I had attended many International Conference, Workshops, and Seminars in the area of Data Science, Python ,Machine Learning And Deep learning Respectively.

Ms.M.E.Sanjana B.E., Student of Computer Science and Engineering at St. Joseph College of Engineering, Sriperumbudur, Chennai, TamilNadu. I had attended National programme on technology enhanced learning in data science and obtained a course completion certificate and also participated in many Workshops and Seminars in