IMPLEMENTATION ON RANKED KEYWORD SEARCH AND DATA ANALYSIS FOR SECURE CLOUD STORAGE

[1]Jujgar Ritika, [2]Rathod.V.U

[1]Students, Department of Computer Engineering,

[2]Prof. Department of Computer Engineering,
Vishwabharati Academy's College of Engineering, Ahmednagar (MH), India

Abstract: Now a day's cloud computing has become more popular, so more information possessors are operated to their information to cloud servers for great comfort and less cost value in data management. In this research paper, the problem of a secure keyword-based search with data analysis using identity-based authentication on the cloud is solved by using encryption of data before outsource to the cloud server. Here, used ranked result based keyword search algorithm for the file search. This System presents those models the network behavior of user sessions across both the front-end web server and the back-end database. In real world example, Most of the people do their transaction through web use. So there are chances of personal figures gets hacked by some malicious users or unauthorized users for that need to provide more security for both web server and database server. For that purpose, the proposed system used duel security on the web server as well as the database server. The dual security system is used to identify & prevent attacks using Intrusion detection system. Duel security prevents attacks and prevents user account data from unauthorized updating database values.

Keywords - secure cloud storage, keyword search, data analysis, data security, encryption, AES, a message digest (MD5).

I. INTRODUCTION

With the development of new computing paradigm, Cloud computing has been considered as a new computing model of enterprise IT infrastructure, which can organize a large number of the resource of computing, storage, and applications, and enable users to enjoy ubiquitous, convenient and on-demand network access from a shared pool of configurable computing resource. Both individuals and enterprises are motivated to send their data to the cloud, instead of purchasing software and hardware to manage the data. Despite the various advantages of cloud services, outsourcing sensitive information like e-mails, personal health records, company financial data, government documents, etc. to remote servers brings privacy concerns. The cloud service providers that keep the data for users may access users‟ sensitive information without authorization process. Data security and privacy concerns have are two major challenges in cloud computing. A general approach to secure data confidentiality is to encrypt the data before outsourcing. Encryption is a fundamental method to protect data privacy in remote storage. However, how to effectively execute keyword search for plaintext becomes difficult for encrypted data due to the unreadability of ciphertext. Searchable encryption provides a mechanism to enable keyword search over encrypted data secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability.

Data security is one of the major worries in the process of cloud computing. Compared to common systems, users will lose their direct control over their data. Data confidentiality is important in data security. In this paper, Explore the problem of integrity verification for large data storage in the cloud. This problem can also be called data auditing when the verification is managed by a trusted third party. Data owner can't trust users as they may be malicious. For that data, owner provides authorization process to the users. And admin provides authorization process to the data owners. For better security, our system combines an additional authorization process for all data owners, and users with the aim of eliminating threats of unauthorized audit challenges from malicious or pretended third-party auditors, which term as admin that is „authorized auditing‟.

II. LITERATURE SURVEY

A. *Multi-Keyword Ranked Search:*

Built up the accessible encryption for multi-keyword arranged explore the farthest point information. In particular, by considering a large number of outsourced reports (information) in the cloud using the importance score and k-closest neighbor methods to build up a beneficial multi-catchphrase search for a plot that can restore the arranged once-over things in the context of the accuracy [1].

A secure, efficient and dynamic keyword search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. In this paper, create a special keyword balanced binary tree as the index, and propose a "Greedy Depth-first Search" algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be holding out to further reduce the time cost. The security is protected against two threat models by using the secure KNN algorithm. The secured KNN figuring is used to scramble the record and demand vectors, and a while later guarantee correct congruity score count between encoded report and question vectors[2].

B. Secure and Lightweight Identity-Based Authentication:

In the cyber-physical cloud environment, Secure and efficient file storage and sharing via authenticated physical devices are

challenging tasks. in this paper, present a lightweight identity-based authenticated data sharing protocol to provide secure data sharing among geographically dispersed physical devices and clients[3]. In the IBADS, there are two phases. First, new data the owner needs to register. Second, the data owner sends an encrypted message to the untrusted cloud service provider using some users‟ devices.

1) Mutual Authentication:
This is one of the most fundamental security attributes required in Cyber-physical systems and generally many other systems. It is assumed that the server may be dishonest or not fully trusted. Specifically, both client and server first complete the authorization process by verifying the authenticity of each other, prior to exchanging any confidential data over public networks.

2) Anonymity:
This allows the hiding of the identity of the client or user, even when an adversary has intercepted some messages from the public channel.

3) Password protection:
The need to ensure password protection in a password-based authentication system is clear, and the client device is usually one of the weaker links. Specifically, the client or user generally uses a low-entropy password to facilitate memorization, and such passwords are vulnerable to password guessing attacks.

4) Impersonation resilience:
Client-server communication protocol runs are executed over an insecure channel, and thus a malicious user can attempt to impersonate as either the client or the server to the other party.

5) Data integrity and confidentiality:
A secure protocol should provide strong data integrity and confidentiality for every transmitted message. Data integrity assures the receiver that the message has not been modified, and confidentiality ensures that only authorized users/devices can have access to the data.

C. Domain and Range Specific Multi-keyword search:

Key to encode the easily breakable information before communicates to the cloud server to keep up protection and security. All standard accessible symmetric encryption (SSE) organizes empower the clients to search for with everything taken into account record report. In this paper, the Domain and Range Specific Multi catchphrase Search (DRSMS) arrange for that compels
the pursuit time and Index storage room. This action handles gathering sort structure to part the report record into D Domains and
R Ranges. The Domain depends upon the length of the watchword and the Range parts inside the space in the context of the fundamental letter of the catchphrase [4].

D. Privacy-Preserving Multi-Keyword Ranked Search:

An observable thought for the multi-keyword ranked search over the encrypted data (MRSE) in light of secure inward thing calculation and in this manner give two essentially improved MRSE plans to successful various stringent necessities in two unmistakable risk models. To improve look incorporation of the information search for advantage and further stretch out these two game plans to help more pursue semantics additionally settled a strategy of strict protestation basics for such a shielded cloud information usage structure. Among different multi-watchword semantics and pick the suitable closeness measure of "sort out arranging," i.e., however many matches as could sensibly be ordinary, to get the over critical of information records to the demand address [5].

E. Dual-Server Public-Key Encryption:

Searchable encryption is of increasing involvement for protecting the data privacy in secure searchable cloud storage. In this paper, the security of a well-known cryptographic primitive, also known as Public Key Encryption with Keyword Search (PEKS) which is very useful in many applications of cloud storage. It has been shown that the traditional PEKS framework pass from constitutional insecurity called inside Keyword Guessing Attack (KGA) developed by the malicious server. To address this security vulnerability, in this paper, a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). As another main contribution, define new different ways of the Smooth Projective Hash Functions (SPHFs) referred to as linear and homomorphic SPHF (LH-SPHF). To demonstrate the feasibility of a new framework, here provided an efficient Manifest of the general framework from a DDH-based LH-SPHF and show that it can achieve strong security against inside KGA [6].

F. *Ciphertext-Policy Attribute-Based Encryption:*

Ciphertext-policy attribute-based encryption (CP-ABE) enables fine-grained access control to encrypted data for corporate applications. In CP-ABE two properties are recently used called traceability and the large universe, greatly enriching the corporate applications of CP-ABE. Traceability is the ability of attribute-based encryption to trace malicious users or

Unauthorized users who intentionally leak the partial or modified decryption keys for profits [7].
In this paper, CP-ABE systems have two advantages:
1) The number of attributes is not polynomially bounded and
2) Malicious users or unauthorized users who leak their decryption keys could be traced. Moreover, another remarkable advantage of the second system is that the storage overhead for traitor tracing is constant, which are suitable for commercial applications.

G. *Encrypted Data in Arbitrary Language:*

Multi-keyword rank searchable encryption (MRSE) systems are constructed based on an algorithm as a k-nearest neighbor for searchable encryption KNN-SE algorithms. In this paper, firstly several serious shortcomings of KNN-SE which limit the practical applications of the existing MRSE systems then proposed a new MRSE system which overcomes all the defects of the KNN-SE based MRSE systems. The new system does not require a predefined keyword set at the system setup phase and support keyword search in arbitrary languages. Use Unicode to encode keywords in arbitrary languages and utilize an efficient way to transform them into encrypted ciphertext. This article proved the security of the system and conducted extensive computer simulations to demonstrate its efficiency [8].

III. PROPOSED METHODOLOGY

A. *Architecture:*

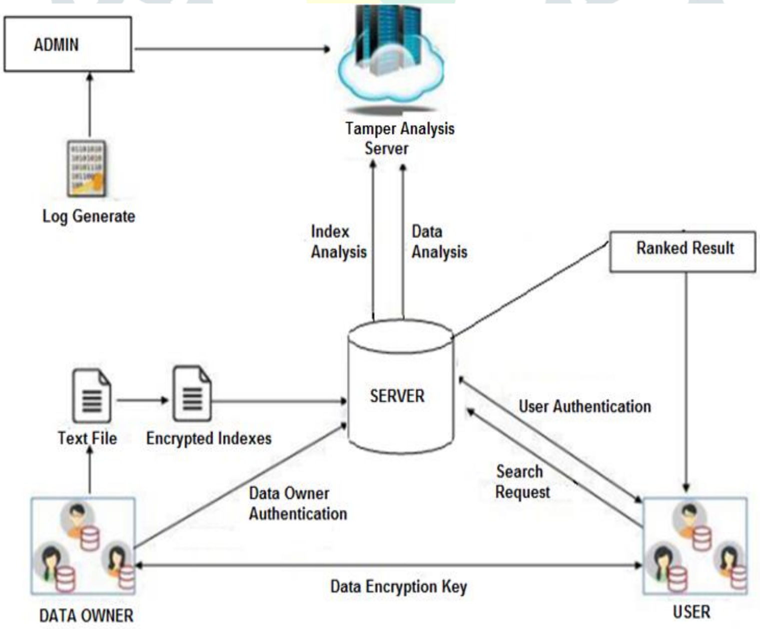

Fig. 1: System architecture

1) *Cloud server:*

Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system. The cloud server is responsible to store the data owner's encrypted files and respond to the data user's search query.

2) Data User

This module first includes the user registration login details then helps users to enter their query keyword to get the most important documents from the set of uploaded documents. The data user can view the uploaded files and downloaded files. The data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search. Then, the keyword is encrypted to a trapdoor using the user's secret key. If the user's attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on the user's search query and finds the match files. Otherwise, the search query is rejected. After the match files are returned, the user runs the decryption algorithm to recover the plaintext.

3) Data Owner:

First, the owner register details and also include login details then Data owner utilizes the cloud storage service to store the files before the data outsourcing; the data owner extracts keyword set from the file and encrypts it into the secure index. The document is also encrypted to ciphertext. After expansion of keywords the data owner support data with encrypting the document utilizing encryption Algorithm and after that upload the encrypted document stored to the cloud server. The data owner to view the uploaded files and downloaded files. The data owner to upload his file with encryption using the advanced encryption standard algorithm (AES). This assures the files to be protected from an unauthorized user.

4) Download Ranked Results:

This module first ensures the user to search the file that is searched frequently using rank search. An authorized user can download the resultant arrangement of documents just if the user is an approved user who has allowed consent from data owner to download a specific document. Data owner allows the authorized user to download the file using his secret key to decrypt the downloaded data. Data owner will send an encrypted secret key to the authorized user to decrypt the document.

5) Searchable Encryption:

Searchable encryption enables keyword search over encrypted data. Searchable encryption permits data owner to outsource
his data in an encrypted manner. Search any keyword without reading the plaintext data becomes difficult for encrypted data due to the unreadability of ciphertext. For that purpose, Searchable encryption provides a mechanism to enable keyword search over encrypted data secure search over encrypted remote data in cloud computing to ensure data privacy and usability.

6) Tamper analysis server:

Admin is the authorized person; admin provides authorization process to the data owners. He checks all the user activity records as well as profile continuously. Admin also watches the data analysis (tampering) on changing the values from the database. In this paper, the MD5 algorithm used for the data analysis and the unauthorized changes made on the databases server.

B. Software Requirements Specifications:

Hardware Requirements

- Pentium IV Processor or above
- RAM 2GB or above
- Hard Disk 100GB and more

Software Requirements

- OS Requirements: Windows 7 onwards
- Netbeans IDE 8.0
- JDK 1.6.0 (JDK 7), Tomcat Apache Server MySQL Server 5.0

C. Algorithms:

1) User Authentication:

Authentication is the process of corroborating the identity of the user. The communication between the user and the server require any authentication. Since the user provides his identity during the communication with the server.

- **Step 1:** The User DU chooses an identity IDc and Forwards it along with the cell number and e-mail id to the cloud server CS. only the parameter IDc is forwarded to the CS securely.

- **Step 2:** Produces an application software by storing Ac = h(ID_c k S_{CS})_h(ID_c k PW_c), where PW_c is the password of DU.

- **Step 3:** Sends a URL link to the e-mail id of the DU and ($PW_{c;}$ W_c) to the cell number of the DU securely, where W_c is the random information.

- **Step 4:** Maintains a list L_U and stores W_c against the public and unique information $TID_{c.}$

- **Step 5:** Login and mutual authentication is Imperative during logging to the CS and the objective is to perform mutual authentication and key agreement.

- **Step 6:** DU get OTP from the CS. The remote the Server checks the time interval Between Time- stamp T and Server receives the message from DU is T1, If (T1 - T) <= ΔT,

  ```
                  DU login successfully.
          Else
                  The CS rejects DU.
  ```

- **Step 7:** User login to the CS and after accomplishing Successful authentication DU has to connect to the CS to Access the Document.

- **Step 8:** On the basis of authentication of tokens, key Generation gives the key to DU and this key is used For decryption of document that is collected from CS.

- **Step 9:** After authentication, DU will collect the Encrypted document from CS and enter their ranked query

  Keyword from the set of uploaded documents. DU search query keyword on encrypted documents stored in the CS.

2) *Ranked Search on encrypted files:*

If the user searches for a one or more than one keyword, there will possibly be many correct matches where some of them may not be useful for the user at all. Therefore, it is difficult to decide to which documents are the most relevant. So for that add the ranking capability to the system by adding extra index information for frequently occurring keywords in a file. Using keyword ranking, the user can recover only the top τ matches where τ is chosen by the user.

- **Step 1:** ranking function is required in order to rank All documents which assign relevancy scores to Each document matching to a given search query.

  ```
  Ranked_Search ()
      For all documents Ri do
  ```

- **Step 2:** metrics used in information retrieval is the Term frequency TF which is defined as the number of times a keyword appears in a document. Instead of using term frequency TF itself, assign relevancy levels based on the term frequencies of keywords.

- **Step 3:** there are η levels of ranking some integer η ≥ 1. Each level stores an index for frequent keywords for Each document. Compare (level1 index of Ri , query index) j = 1

- **Step 4:** i^{th} level index incorporate all keywords in the (i + 1) th level and the keywords that have term Frequency for the i^{th} level.

  ```
    while match do
          Increment j
          Compare (level j indices of Ri , query index)
    end while
  ```

- **Step 5:** The higher the level, the higher the term The frequency of the keywords.

  ```
    Rank of Ri = highest level that match With query index
    end for
  ```

All the keywords that exist in a document are included in the first level search index. The other higher level indices incorporate the frequent keywords that also present in its previous level, but this time they have to present the number of times, which are at least the term frequency of the consistent level.

- **Step 6:** DU enter their ranked query keyword to get The most important documents from the set of Uploaded documents. DU search query keyword on encrypted documents stored in the CS.

- **Step 7:** Ifthe DU‟‟s attribute set fulfill the access the Policy defined in the encrypted document. The CS responds on DU‟‟s search query and finds the match documents. And these encrypted documents are decrypted to recover the plaintext.

```
else
        The search query is rejected.
```

3) *AES Encryption Process:*

KeyGenCE (M) → K is the key generation algorithm that maps a data copy M to a convergent key K;
EncCE (K, M) → C is the encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs ciphertext C;
DecCE(K, C) → M is the decryption algorithm that takes both the ciphertext C and the convergent key K as inputs and then outputs the original data copy M;
TagGen (M) → Maps the original data copy M and outputs a tag T (M). Where T(M) is the tag generation algorithm.

- **Step 1:** Data owner Select File
- **Step 2:** Encrypt File

```
For encryption of data:-

        R= Read (input file),
        K=Key generation (file)
        E=Encrypt (file, key),
        encode the upcoming file
        C=Convert (file),
If (encrypt), then file convert plain to cipher text
```

- **Step 3:** Upload Encrypted file on the cloud or store the file on secondary storage.
- **Step 4:** User search the file available on the cloud or secondary storage.

```
D=Decrypt (file), decode the file
If (decode), then file convert ciphertext to plaintext
Else, file not decoded
```

- **Step 5:** If found then retrieve to the user and maintain the index**.**
- **Step 6:** Identity identified
- **Step 7:** Download file
- **Step 8**: Stop.

4) *MD5 Algorithm:*

The main message digest 5 (MD5) is a hashing algorithm which processes data in 512-bit blocks .this 512 bit blocks are broken down into the 16 words composed of 32-bits each. So the output from MD5 is a 128-bit message digest value. The Message Digest 5 (MD5) process is used to analysis database modification result which is as follows:
Input - input data D = {D1, D2, D3, Dn} saved into the hash table.

- **Step 1**: Arrange all input data D into the matrix Format and saved into the Log files.
- **Step 2:** Consider a selected data m act as a new selected data.
- **Step 3:** position m gets changed after allocated Time period.

- **Step 4:** If data get hacked or leaked by some Malicious users**.**
- **Step 5:** Data leakage occurs.
- **Step 6:** To analyze the leakage data and Prevent using the data analysis (tamper analysis).
- **Step 7:** To get original data to call the revert Back function.
  Step 8: When the user calls that dishonest file, hash Function gives to the user a previous data. And log File maintained at the admin side.
- **Step 9:** Return True.

Output - The hashed value is changed then the log will generate.

D. Mathematical Model:

The Proposed System can be mathematically represented as follows:

Set (S) = {I, O, F, S1, S2}
Where,
S = System.
I = Input (Incoming owner requests of the file).
O = Output (Authentication using identity and Detect
Tampering).
F = {f1, f2, f3, f4}.
Where,
f1 = Encryption for upcoming
file. f2 = Identity generation of
each user. f3 = Tampering
detection from DB. f4 = Log
generation.
S1 = Initial state is the state in which the system is waiting for incoming user
requests. S2 = Final state is the detect tampering and restored successfully.

As for storage on database mathematically can be represented as follows:

Input: Function DATABASE Tamper DETECTION ()

Set (V) = {V0, V1, V2, V3, V4, V5}
Where,
V0 = Get the time in seconds (T)
V1 = Visit Database table for reach interval of
T
V2 = Get a record from the database
V3 = Hash it using MD5
Algorithm
V4 = Create a vector of hash
values
V5 = Send to Notarize

Output:

VALIDATOR: (Here this module is responsible for periodically scans the audited tables, computing the hash values on a per transaction basis).

- **Success Conditions:** when do not change any value from the database.
- **Failure Conditions:** system fails when the attackers get success form database insertion.

User Authentication mathematically represented as follows:

In this paper, the authentication process allows the system to identify the user through a username and then validate their identity through a password. There are even stronger methods of the user authentication such as one-time passwords (OTP).

Whenever a user logs in the system, user will be provided with a new password this is usually provided by the system itself. This password will generate random numbers. Each time a new password is created for any particular user, the previous password for that user will be removed from the system. And a new password will be updated for that particular user. Only one single password used for once login. The password will be sent to the authorized user's mail account. Therefore, at the same time cloud server checks the validity of the user. As a result, only an authorized user with a valid mail account will be able to connect to the cloud server.

Set (U) = {U1, U2, U3, U4, U5, U6}

Where,

U1 = Registration phase
U2 = Authentication phase
U3 = user get OTP from the server
U4= the remote server checks the time
interval between Timestamp T and
server receives The message from user
T1,
U5 = Verification of the
message U6 = User login
phase

- **Success Conditions:** If $(T1 - T) <= \Delta T$, then user login successfully.
- **Failure Conditions:** the server rejects user.

Ranked keyword search mathematically represented as follows:

Set (R) = {R1, R2, R3, R4, R5, R6, R7, R8, F5}
Where,

R1 = User authentication and login
R2 = search query keyword on encrypted Documents stored in the cloud server.
F5 = Function Ranked_Search ()
R3 = Compare with all documents index uploaded to The cloud server
R4 = Number of times keyword appear
R5 = Store index count for frequent query keyword for Each search document
R6 = Increment count
R7 = Highest level match with query index
R8 = decrypt and download the document

- **Success Conditions:** The cloud server responds on the user's search query and finds the match documents and these encrypted documents are decrypted to recover the plaintext.
- **Failure Conditions:** The search query is rejected.

V. RESULT AND DISCUSSIONS

The web application that communicates with the local server and Trust Server using REST API. The evaluated time required for search file using tag generation and file encryption. Here also calculate the file modification using the message digest algorithm.

TABLE 1: PRECISION TABLE

Input Keyword	Total number of files retrieve	Relevant Files	Precision

Network Security	Network Security, Network Security Model, Network Security Model, Security Testing	3	75%
Java	Java, Java Programming, Java Tutorial, Java Software	4	100%
Encryption Decryption	Encryption, Decryption	1	100%

Used precision to measure the result accuracy. To generate the fuzzy keyword search, randomly choose keywords and modified it into a fuzzy keyword. An important parameter in our scheme is the number of the keywords in the query searched by the users. The main reasons for the enhance the accuracy were the use of the new method for the keyword transformation and the threshold T. The precision of the exact match very small amount decreased as the number of the query keywords increased from 1 to 10. Table 2 shows the index tree building cost compare the time cost of base paper and mine.

TABLE 2: TIME OF INDEX TREE CONSTRUCTION

	Time of index tree construction	
No of documents in the collection	Base Paper (Sequential)	Proposed System (Parallel)
5	5	1.60
10	10	2.50
15	15	2.78
20	20	3.50
25	25	3.90

This solution could return not only the exactly matched files but also the files including the terms semantically related to the query keyword. Parallelized index construction using multi-threading for fast index tree generation. the efficiency of our proposed scheme demonstrates Experimental results.

1. **Keyword Search graph:**

TABLE 3: MOSTLY VISITED RANKED FILES

FILE NAME	**HIT COUNT**
test.des	20
upload.des	8
get_data.des	2
add_data.des	2
file.des	1

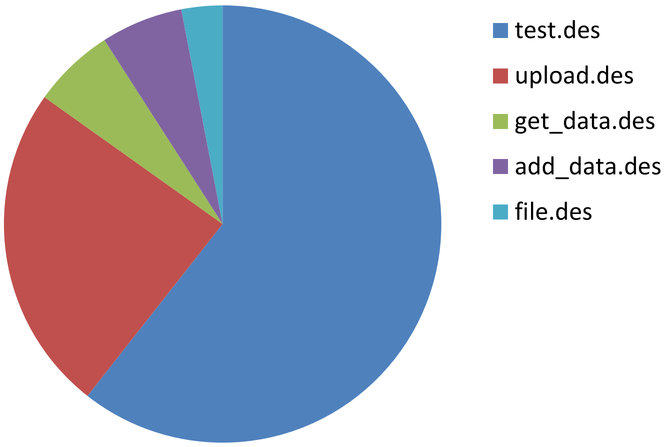

Fig. 2: Number of Mostly Visited Files Record

2. Data Analysis Graph:

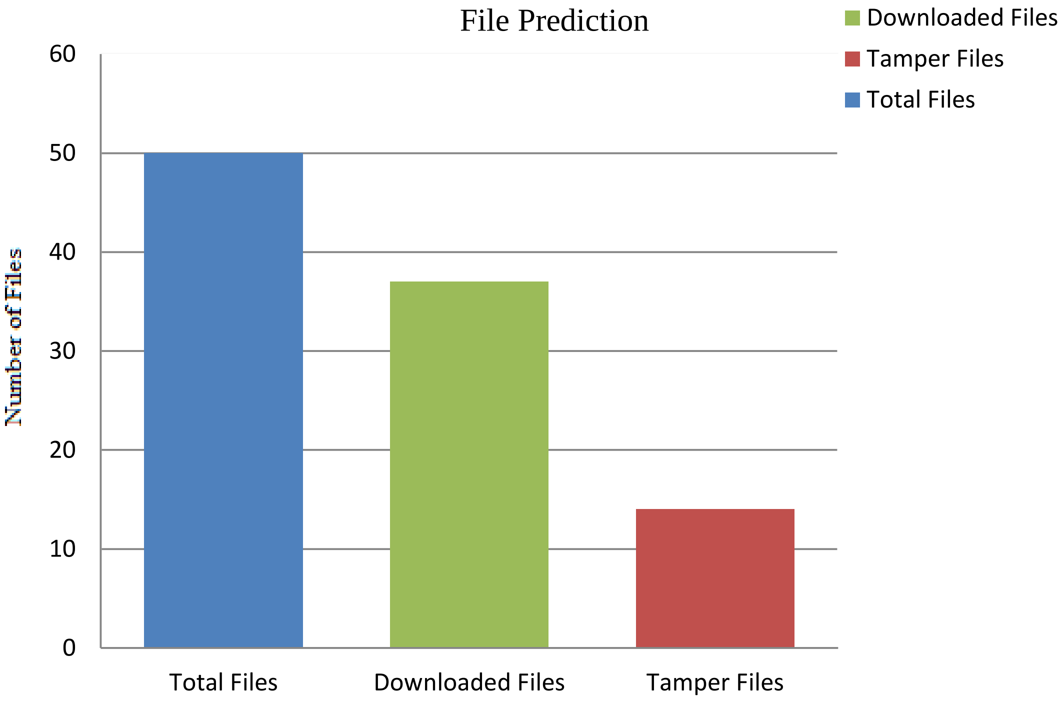

Fig. 3: Number of tamper files out of total file

VI. CONCLUSION

In this paper, Secure and efficient ranked result based keyword search which supports not only the keyword ranked search but also allows the hiding of the identity of the user, Our proposed technique provides dual security using data encryption and data analysis that is tamper analysis server in the cloud environment. Data encryption is done on the web server and the data analysis is done at the database server. Here presents a relative addressing method in which data will check at entry level when user uploading phases using data analysis. In future work to design a dynamic searchable encryption scheme whose updating operation is performed by a cloud server.

VII. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. I wish to thank all our friends and well-wishers who supported us in completing this paper successfully. I sincerely thank my Department

Head, PG coordinator, and all the other staff members to give me the guidelines for this paper. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] H. Li, D. Liu, Yuanshun Da, T. H. Luan, Xuemin, Shen, "Enabling Efficient Multi-Keyword Ranked Search Over Encrypted Mobile Cloud Data Through Blind Storage", *IEEE Transactions On Emerging Topics In Computing, Volume 3, No: 1*, pp: 127-138, March 2015.

[2] K.S.Saravanan, S. Karthika, "A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 5, Issue 2, pp: 244-247, February 2016.

[3] A.Karati, R.Amin, S. H. Islam, Kim-Kwang R.C, "Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment", *IEEE Transactions on Cloud Computing*, Volume 3, No: 1, May 2018.

[4] Raghavendra S, Geeta C M, R. Buyya, Venugopal K R, S Iyengar, L M Patnaik, "DRSMS: Domain and Range Specific Multi-Keyword Search over Encrypted Cloud Data", *International Journal of Computer Science and Information Security* Vol. 14, No. 5, pp: 69-78, May 2016.

[5] A.K.Narayankar, G.Rathod, S.Londhe, A.Wankhade, M.A. Ansari, "A Review on Privacy-Preserving Multi Keyword Ranked Search over Encrypted Cloud Data", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol.5, pp: 3532-3537, March 2016.

[6] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, "Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage", *IEEE Transactions on Information Forensics and Security, vol.11, no. 4, 789-798, 2016.*

[7] J.Ning, X.Dong, Z. Cao, "White-Box Traceable Ciphertext- Policy Attribute-Based Encryption supporting Flexible Attributes" *IEEE Transactions on Information Forensics And Security, Vol. 10, No. 6, June 2015.*

[8] Y. Yang, X. Liu, R.H. Deng, "Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language" *IEEE Transactions on Dependable and Secure Computing, published online, DOI:10.1109/TDSC.2017.2787588, 2018.*

[9] X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. "An efficient privacy-preserving outsourced calculation toolkit with multiple keys." *IEEE Transactions on Information Forensics and Security* 11.11 (2016):2401-2414.

[10] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, "Protecting Your Right: Verifiable Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, 2016, vol. 27, no. 4, pp. 1187-1198.

[11] Y. Yang and M. Ma, "Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds," *IEEE Transactions on Information Forensics and Security*, 2016, vol. 11, no. 4, 746-759.

*[12]*Y.Yang Member, X.Liu, X. Zheng, C. Rong, W. Guo, "Efficient Traceable Authorization Search System for Secure Cloud Storage" *IEEE Transactions On Cloud Computing DOI 10.1109/Tcc.2018.2820714.*