International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

GDFS based data encryption technique in cloud computing environments

M. Lawanya Shri[*1], M.B. Benjula Anbu Malar[2],

G.Priya[3], M.Deepa[4], K. Santhi[5]

[1,2,3,4,5]*SITE, VIT University, Vellore, Tamilnadu, (India)*

ABSTRACT

The data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values.We construct a tree-based index structure and propose a "Greedy Depth-first Search (GDFS)" algorithm based on this index tree. The data owner is responsible for generating updating information and sending them to the cloud server. In the modification process, of this Project is Data is encrypted, split and stored in separate Servers. Data owner encrypts the data and index using AES encryption with secret key are sends to cloud server. Also data owner sends the secret and symmetric keys to data user for authentication and decryption process. Also we use replica server for code backup and recovery.

Keywords: Cloud Computing , Greedy Method, Cloud Server, Encryption ,Decryption

I.INTRODUCTION

Cloud computing is a model for allowing ubiquitous, convenient, and on-demand network access to a number of configured computing resources. Cloud computing has a number of favorable aspects to address the rapid growth of economies and technological barriers. Cloud service models typically consist of PaaS, SaaS, and IaaS. PaaS, such as Google's Apps Engine, Salesforce.com, Force platform, and Microsoft Azure.SaaS, such as Google Docs, Gmail, Salesforce.com.IaaS, such as Flexiscale and Amazon's EC2. Private clouds are dedicated to one organization and do not share physical resources. The resource can be provided in-house or externally. Public clouds share physical resources for data transfers, storage, and processing. However, customers have private visualized computing environments and isolated storage. Hybrid Cloud architecture merges private and public cloud deployments.

1.2 Cloud Setup

Cloud Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the user information to authenticate the user when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Cloud Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job. The Request of all the Users will process by the Resource Assigning Module. To communicate with the Client and with the other modules of the Cloud Network, the Cloud Server will establish connection between them. For this Purpose we are going to create a User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Resource Assign Module in Fist in First out (FIFO) manner.

In the proposed system,the data owner needs to store the threshold value and unencrypted index tree and the information that are necessary to recalculate the IDF values.We construct a tree-based index structure and propose a "Greedy Depth-first Search (GDFS)" algorithm based on this index tree. The data owner is responsible for generating updating information and sending them to the cloud server.

In the modification processof this project is data is encrypted, split and stored in separate servers. Data owner encrypts the data and index using AES encryption with secret key are sends to cloud server. Also data owner sends the secret and symmetric keys to data user for authentication and decryption process. Also we use replica server for code backup and recovery.

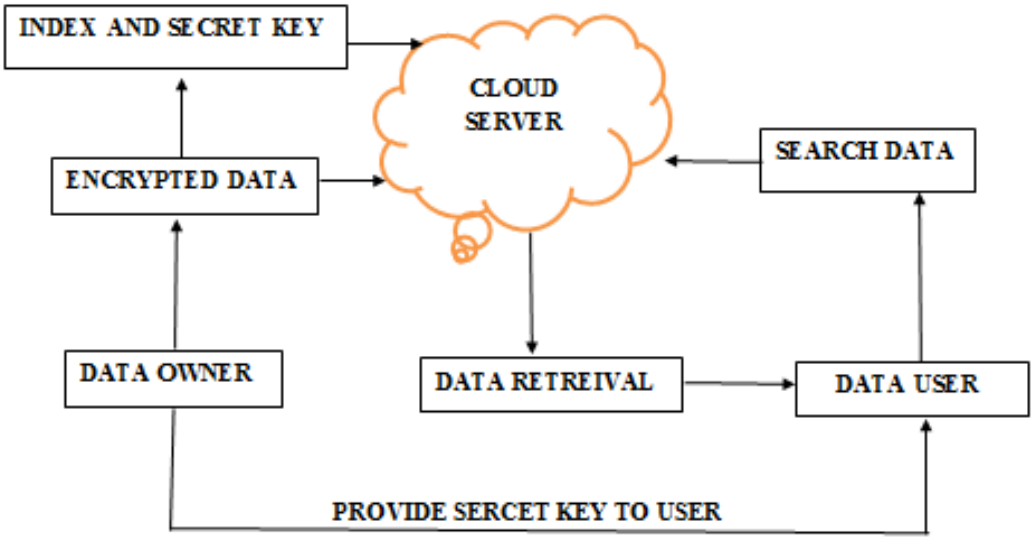

Fig. 1 Architecture Diagram

Cloud Server Deployment

Cloud Server is the major main server which contains the index data of the entire data present in all sub Cloud Servers. The Cloud Server will act as the main server to receive the query from the user. The user query is encrypted using AES algorithm, and sends to the main Cloud Server. The main Cloud Server decrypts the query and match with the index data present in it. The main Cloud Server will find the best match file using ranking algorithm.

Filtering Keyword Based Stemming Algorithm

The words in the files are filtered and main keywords are filtered using Stemming Algorithm. The main keywords are extracted to filter the unwanted words. The Files names are updated in the corresponding cloud servers.

Encryption Module

The query of the user is encrypted using AES algorithm. This encryption process will prevent the data theft from the hackers. Data security is ensured using AES encryption.

Ranking Algorithm Module

In this module we rank the best file by calculating the ratio between term frequency with the total number of keywords. The value is calculated and compared with the rest of the values. The maximum valued files are ranked in order. The files are retrieved to the user as the index data of all the files are maintained in the index of the main cloud server.

Best File Identification

The best file identification is achieved using Top k Query Algorithm. The maximum ranked values are obtained using Term frequency calculation. The files are kept in the ascending order. The best files are given as output to the main cloud server. The main cloud server retrieves top files and given as output to the user.

Trusted Party Auditor

Once added the parity added bits, then the data will be given to the Trusted Parity Auditor. The Trusted Parity Auditor will generate the signature using change and response method. The data will be audited in this module, if any changes occur it will provide the intimation regarding the changes.

Replica Storage

We will maintain the separate Replica Cloud server. If suppose the data in the data server was lost, then the Main Cloud server will contact the Replica Cloud server and get the data from the Replica Cloud Server. By using this concept, we can get the data if any data loss occurs.

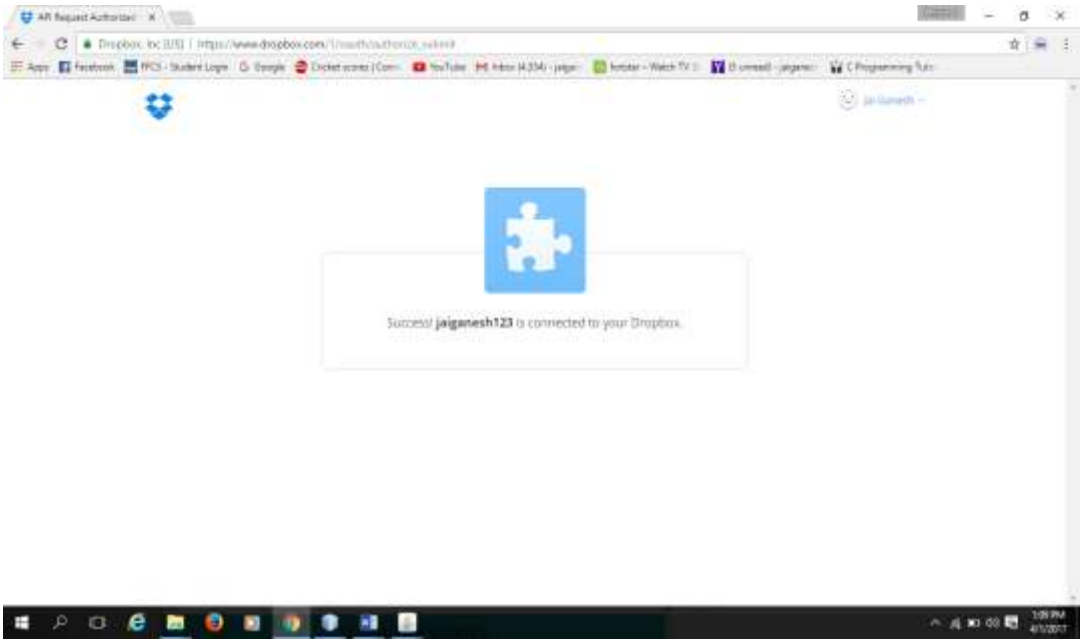

Fig 5.1 Dropbox connection

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fig 2 Admin Cloud Server

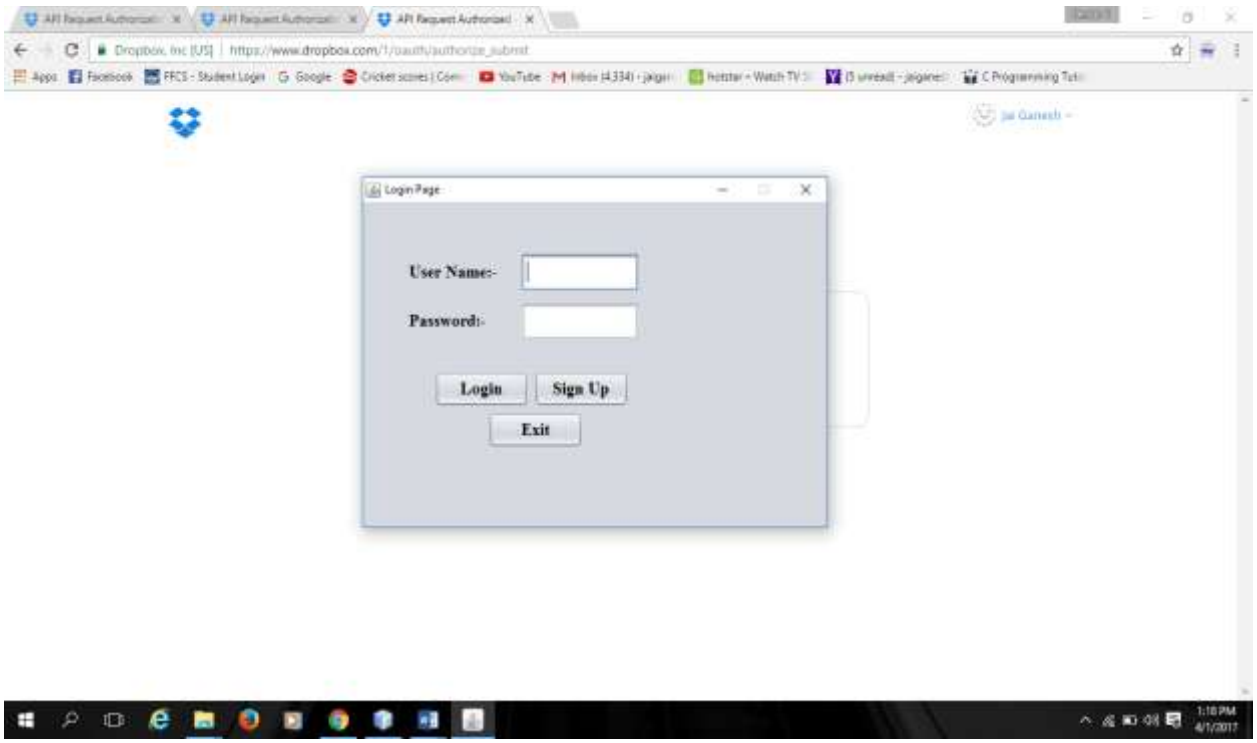

Fig 3 User Login

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

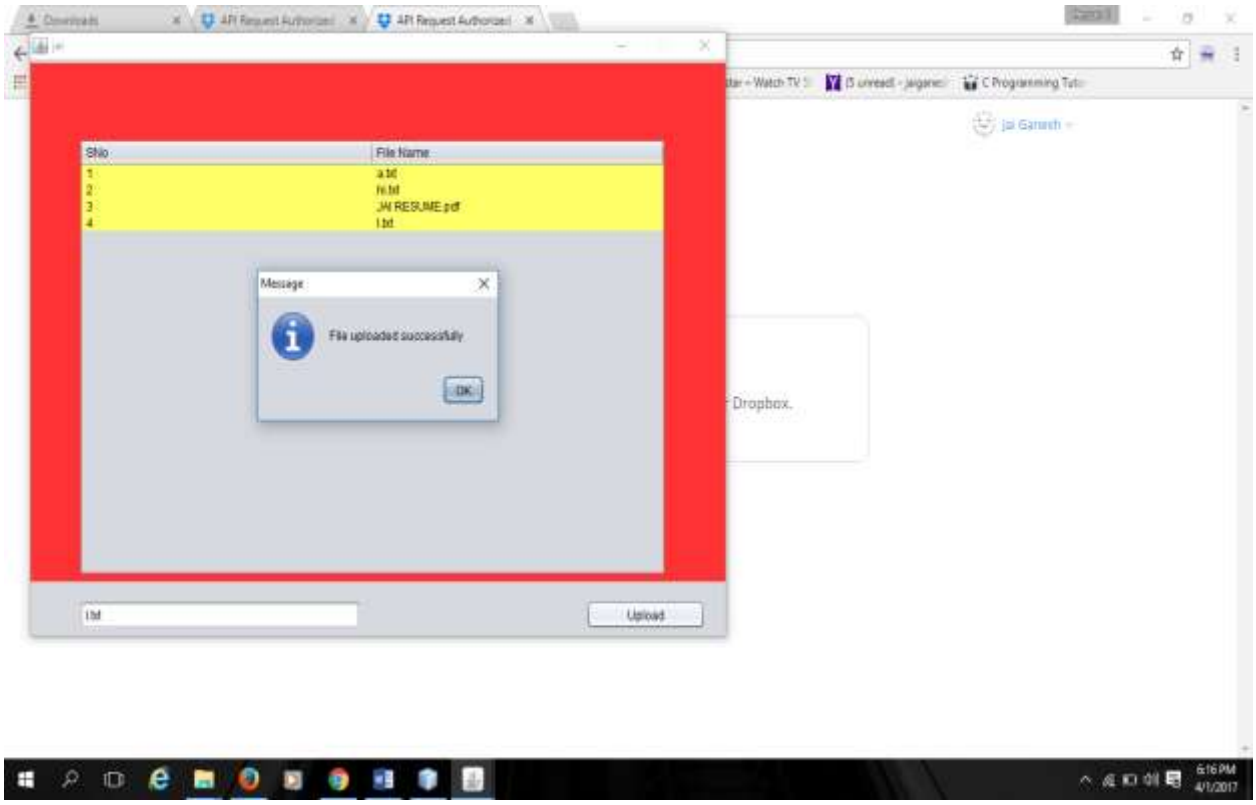

Fig 4 File Upload

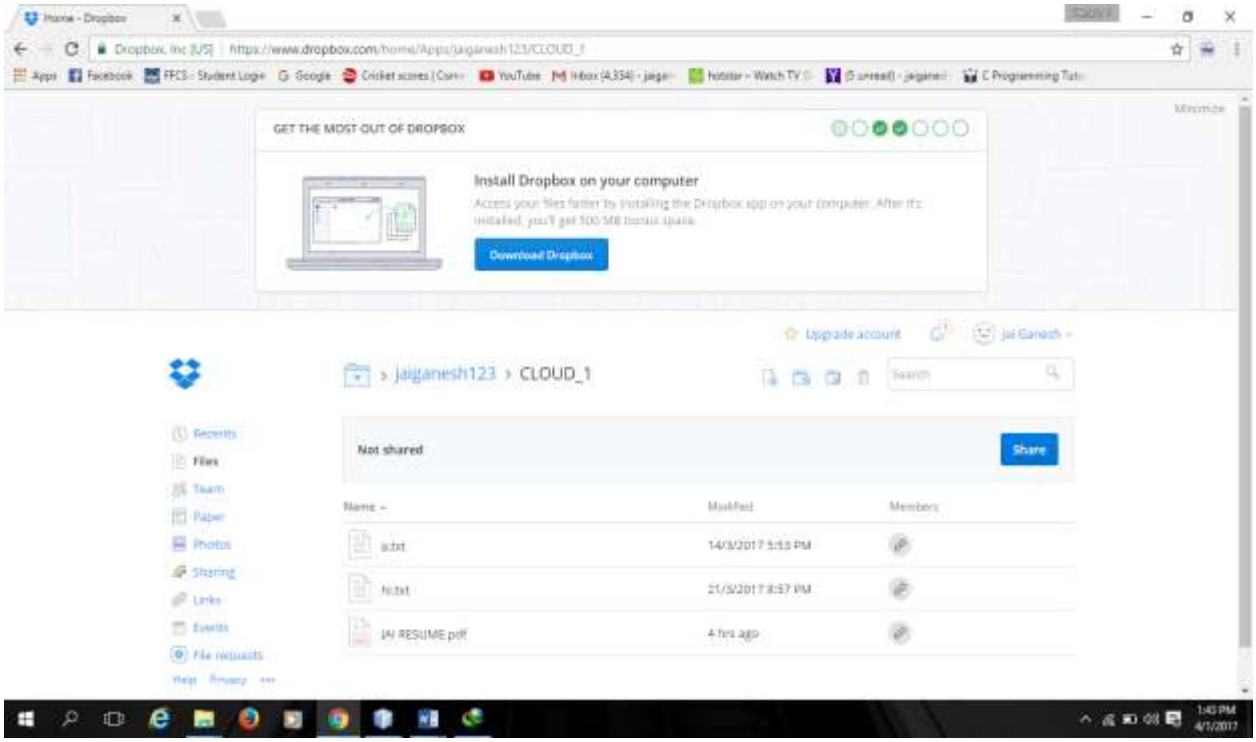

Fig 5 File Uploaded in Cloud

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

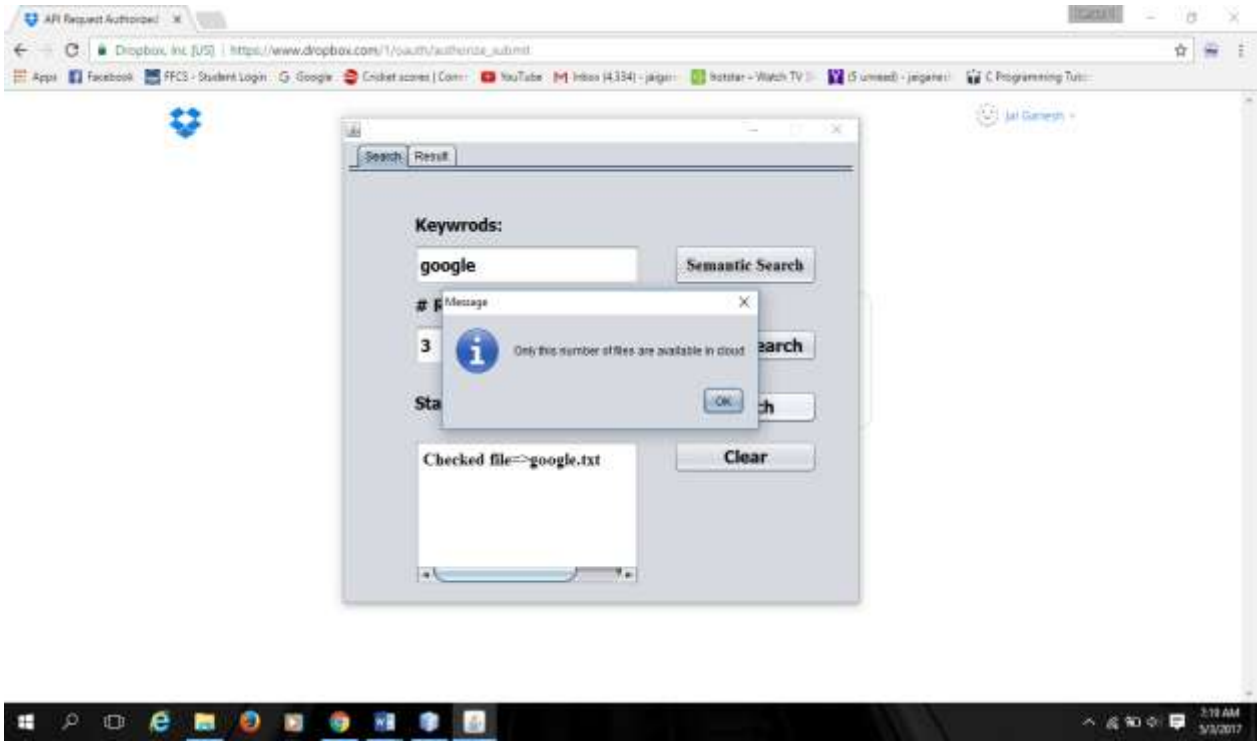

Fig 6 Keyword Search

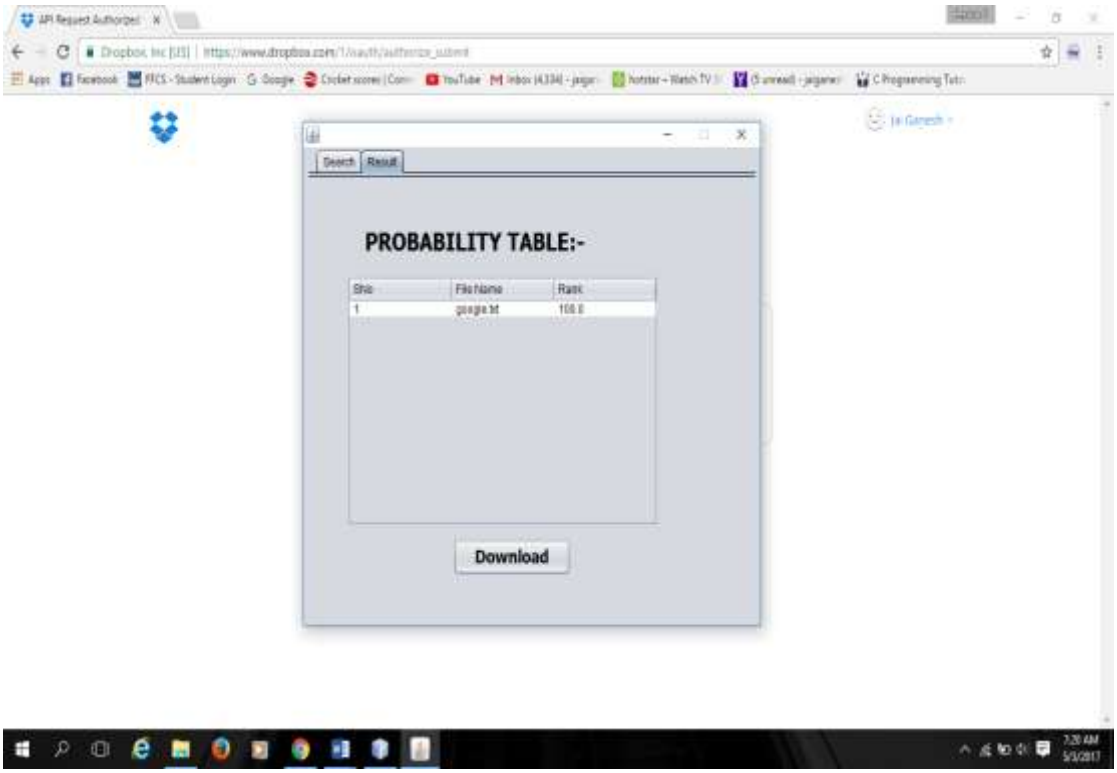

Fig 7 Probability Table

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 11, November 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

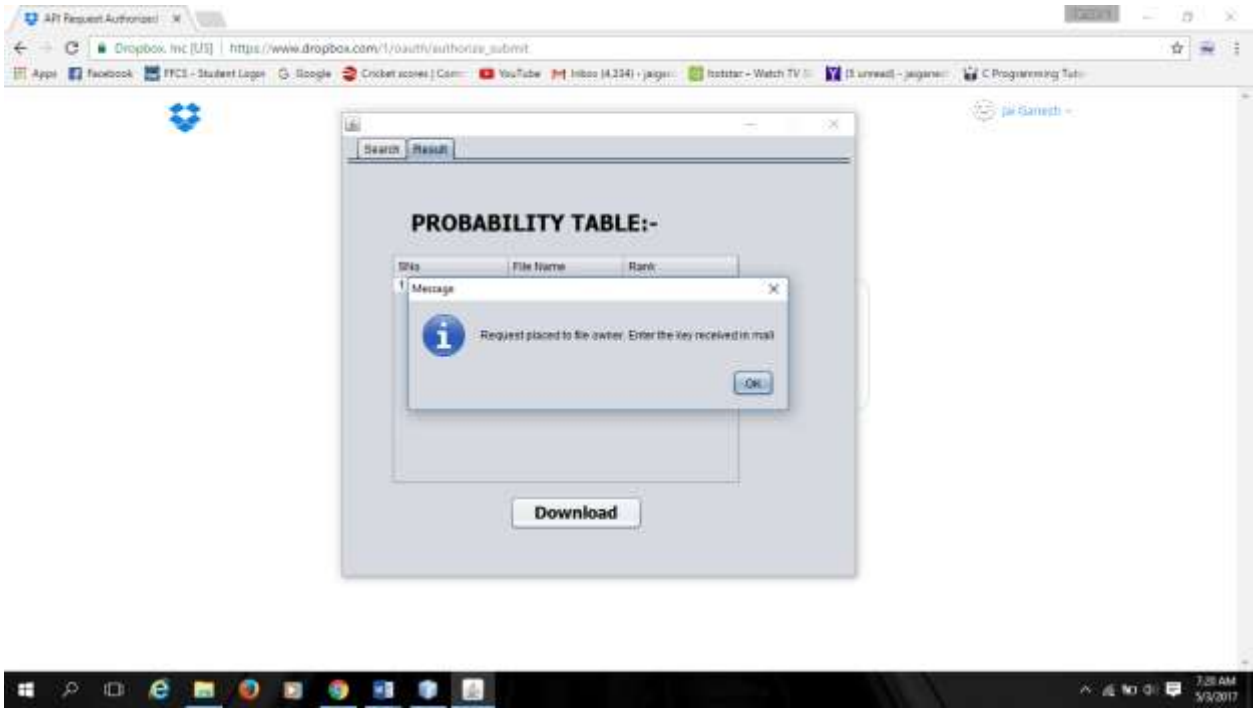

Fig 8 Downloading File

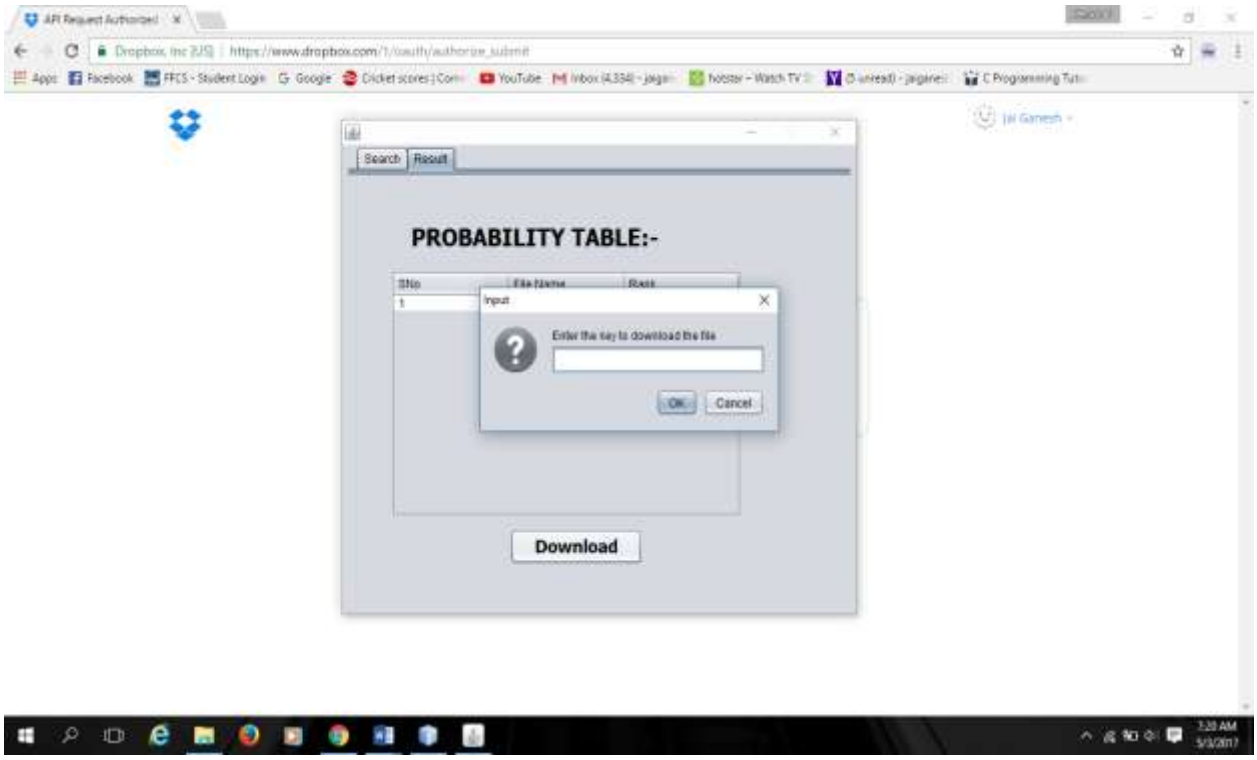

Fig 9 Key for Download

II.CONCLUSION

In this paper, a secure, efficient and dynamic search schemeis proposed, which supports not only the accurate multikeywordranked search but also the dynamic deletion of documents. We construct a special keyword balancedbinary tree as the index, and propose a "GreedyDepth-first Search" algorithm to obtain better efficiencythan linear search. In addition, the parallel search processcan be carried out to further reduce the time cost. The security of the scheme is protected against two threat models byusing the secure kNN algorithm. Experimental results demonstratethe efficiency of our proposed scheme. There are still many challenge problems in symmetric SEschemes. In the proposed scheme, the data owner is responsiblefor generating updating information and sending themto the cloud server. Thus, the data owner needs to store theunencrypted index tree and the information that are necessaryto recalculate the IDF values. Such an active data ownermay not be very suitable for the cloud computing model.

REFERENCES

[1] Mikhail Strizhov and Indrajit Ray, -"Multi-keyword Similarity Search Over Encrypted Cloud Data", Transactions on Data Privacy, Volume 9 Issue 2, August 2016.

[2] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou,-"Privacy-Preserving Multi-keyword Search over Encrypted Cloud Data" IEEE transactions on parallel and distributed systems, Volume 25, No. 1, January 2014.

[3] CengizOrencik, Murat Kantarciogluy and ErkaySavas –"A Practical and Secure Multi-Keyword Search Method over Encrypted Cloud Data", 2013 IEEE Sixth International Conference on Cloud Computing, December 2013.

[4] Bing Wang, Shucheng Yu, Wenjing Lou and Y. Thomas Hou-"Privacy-Preserving Multi-Keyword Fuzzy Search over Encrypted Data in the Cloud", INFOCOM, 2014 Proceedings IEEE, July 2014.

[5] Shri, M. L., & Subha, D. S. (2013). An implementation of e-learning system in private cloud. *International Journal of Engineering and Technology*, *5*(3), 3036.

[6] LawanyaShri, M., Subha, S., & Balusamy, B. Energy-Aware Fruitfly Optimisation Algorithm for Load Balancing in Cloud Computing Environments. *Int J IntellEngSyst*, *10*(1), 75-85.

[7] Jothipriya, G., & Shri, M. L. (2013). Database Synchronization of Mobile-build by using Synchronization framework. *International Journal of Engineering and Technology*, *5*(3), 2316-2321.

[8] Malar, M. B. A., Shri, M. L., Deepa, M., &Santhi, K. (2016). Approach for Secure Authorized Deduplication using Hybrid Cloud. *International Journal of Applied Engineering Research*.

[9] Lawanyashri, M., Balusamy, B., & Subha, S. (2017). Energy-aware hybrid fruitfly optimization for load balancing in cloud environments for EHR applications. *Informatics in Medicine Unlocked*.

[10] LawanyaShi, M., Balusamy, B., & Subha, S. (2016). Threshold-Based Workload Control for an Under-Utilized Virtual Machine in Cloud Computing. *International Journal of Intelligent Engineering and Systems*, *9*(4), 234-241.

[11] M. B. BenjulaAnbu Malar, M. Lawanya Shri, M. Deepa3, K. Santhi "Approach for Secure Authorized Deduplication using Hybrid Cloud ",INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH,2016.

[12] K.santhi, M.deepa, M.Lawanyashri, M. B. Benjulaanbu malar "an efficient active audit services for achieving data integrity in cloud system", international journal of pharmacy & technology,2016.

[13] S. pavithra , M. lawanyashri, "privacy preserving the electronic health record using encryption protocol in cloud computing", international journal of pharmacy & technology,2016.

[14] M. Lawanya Shri, M.B.BenjulaAnbumalar, K. Santhi, Deepa.M ,, E-Learning System With Hierarchical Attribute Set Based Encryption Access Control In Cloud" ", International Journal Of Pharmacy & Technology,2016