

## Encrypted graph based Keyword searching Technique

Snehal Aher<sup>1</sup>, Meghangi Amrutkar<sup>2</sup>, Pallavi Garud<sup>3</sup>, Pranali Pawar<sup>4</sup>,  
(<sup>1,2,3,4</sup>.BEIT, Dept. of Information Technology, KKWIEER,Nashik)

**Abstract:** In this era cloud computing is widely used by many users, so the computing and storage services are moving from cloud to edges. In edge computing, data is processed by the device itself or by a local computer or server, rather than being transmitted to a data centre. To deal with this problem the proposed system provides solutions of data encryption at data owner side before outsourcing. If data owner is valid then cloud service provider will send the tokens to data owner and data owner will be able to outsource the data. Also, user can find appropriate file by using keyword search rather than searching by file name. The proposed system provides a searching technique called K-Nearest Keyword searching algorithm to search the file keyword instead of file name. If any user wants to read or access the data, the user will send request to data owner. At the time of registration user will be authenticated by service provider using K-Map method. After the confirmation of valid user, service provider sends request to data owner for accessing data and approval will be given by data owner. Then user will be able to download the original data by using K-Map secret key.

**Index term:** Keyword searching, edge computing, K-Map

### I. Introduction

Data outsourcing has become an important application of cloud computing and edge computing, as data owners free themselves from maintaining IT infrastructure and data management. It has been acknowledged that security issues have become the biggest challenges towards cloud computing. The trend that computation and storage services are moving from clouds to edges further highlights data privacy issues, because privacy risks at the edge side might be even greater than the cloud side. To protect data privacy, data owners should encrypt data before outsourcing. However, traditional encryption techniques make outsourced data no longer query able, which would severely impact on data usability. Though a lot efforts have been made to enable keyword search on encrypted textual data how to perform various queries on encrypted graph structured data is still a challenging problem.

### II. Material And Methods

**Work flow of system:** An web application is consists of three main modules upload file module, search keyword module and download file module.

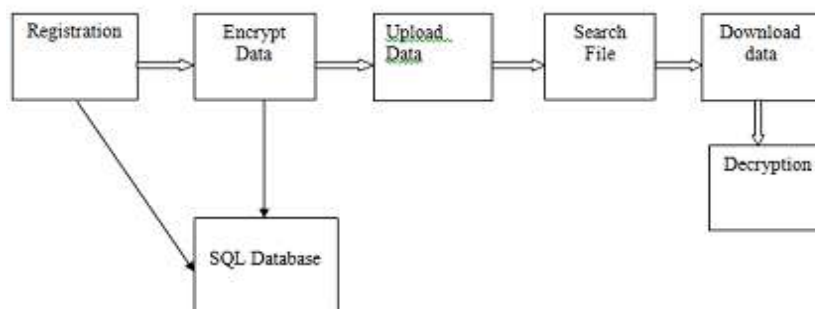


Figure 2: workflow of system

This system consists of 4 modules such as:

1. Registration module
2. Login module
3. Upload file module
4. Search file module
5. Download file module

### **Registration Module**

- User has to first register in our system by filling necessary details.
- This module contains following fields:
  - i. Username.
  - ii. Password.
  - iii. Mobile No.
  - iv. Email.
- After registration user have to click on submit button and then request will be send to admin.

### **Login Module**

- After the permission given by the admin user can login to system any time.
- For login, first user has to enter username.
- After that enter the password.
- Then, user will click on “login” button.
- If user enters everything correctly then he/she can login to system.

### **Upload File Module**

In this module user upload his/her file. The uploaded file is encrypted format. In this encryption process we are implementing AES (Advance Encryption Standard).The uploaded file is not stored into the cloud server. In this system, we implemented the integrity for Uploaded data every time.

- After login into system we can upload files.
- For uploading files we have to first click on upload file option then we have to browse the path of file which we want to upload.
- Set the Graphical Password.
- Then click on upload file button to upload file.
- Users can upload as many files as they want.

### **Search File Module**

User can search the file related to the content they have been entered.

User have to perform the following steps:

- Enter the key (content) present on the file.
- Click on ”Search ” button.
- Related to key files will be displayed.
- Select the file to be needed.
- Then file request will be send to the admin.

### **Download File Module**

User can download only those files that are been accepted by the admin.

User have to perform the following steps:


- Click on “click here” option related to file you want to download.
- After that click on image to enter the graphical password.
- Then click on download button and file will get downloaded.

## **III. Result**

**I. Upload file:** K-map algorithm is used for uploading file on cloud. While uploading a file there will an image on which data owner will select two points it will automatically generates it’s coordinates and these coordinates will be used as secret key. For further accessing of file, data owner must remember these coordinates or point where he has clicked over the image.

Client Name:

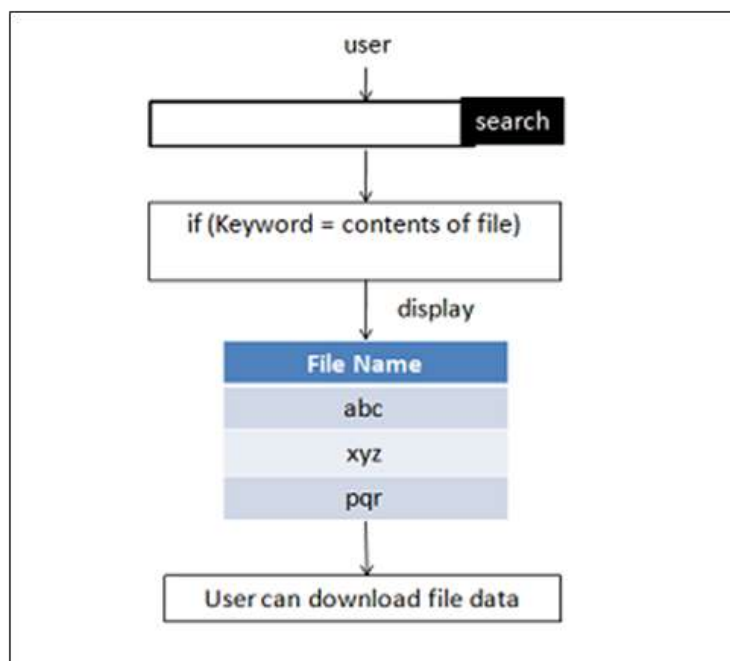
Click on the image to set Graphical Passwords



First Co-Ordinate Point:  
 X:   
 Y:

Second Co-Ordinate Point:  
 X:   
 Y:

**II. File searching and downloading:** User can search file by keywords which contains within file instead of searching file by its file name. For that purpose Top K- nearest keyword searching [KNK] technique is used. Which match nearest keyword to find appropriate result. When user enters the keyword to search a file, that keyword will be compared with the contents of each file stored on cloud. If appropriate match found, then system will displays list of files. If user wants to download any of the file, then he/she have to take permission from data owner and cloud service provider. After the confirmation of valid user, service provider sends request to data owner for accessing data and approval will be given by data owner. Then user will be able to download the original data



#### **IV. Conclusion**

Data is outsourced by the data owner in the original format on server. The data is encrypted/ decrypted at server side and it uploaded to the cloud, which takes overhead for processing of data on cloud server. The main disadvantage of existing system is data owner has no control over the data and has completely trusted with cloud service provider. To deal with this problem the proposed system provides solutions of data encryption at data owner side before outsourcing and this system provides high security, integrity. So, this system can be useful to everyone who wants to upload confidential data and require high security.

#### **References**

- [1]. I. Abraham, D. Delling, A. V. Goldberg, and R. F. Werneck. Hierarchical hub labelings for shortest paths. In Algorithms–ESA, pages 24–35. Springer, 2012.
- [2]. R. Agarwal, P. Godfrey, and S. Har-Peled. Approximate distance queries and compact routing in sparse graphs. In IEEE INFOCOM, pages 1754–1762, 2011.
- [3]. T. Akiba, Y. Iwata, and Y. Yoshida. Fast exact shortest-path distance queries on large networks by pruned landmark labeling. In ACM SIGMOD, pages 349–360, 2013.
- [4]. B. Bahmani and A. Goel. Partitioned multi-indexing: bringing order to social search. In WWW, pages 399–408, 2012.
- [5]. J. Blocki, A. Blum, A. Datta, and O. Sheffet. Differentially private data analysis of social networks via restricted sensitivity. In ACM ITCS, pages 87–96, 2013.