Top-K Closest Keyword Exploring Queries by Using Graph Encryption

Aishwarya.N[1], Geetha.P[2], Haritha.K[3], Keerthana.S[4]

[1,3,4]UG Scholar, [2]Assistant Professor
Department of CSE
Dhanalakshmi College of Engineering

Abstract—For the purpose of security demands in cloud application, client encrypt's the data before storing into the cloud. To properly encrypt the data, graph encryption is used because edges and clouds are not trusted. For retrieving data, query search is done in encrypted graph structured data. We store necessary information using several indexes in graph structure for answering queries.We can easy identify the related information using top-k closest keyword search.

Index Terms—Graph Encryption, Cloud Computing, Top-k closest keyword.

I. INTRODUCTION

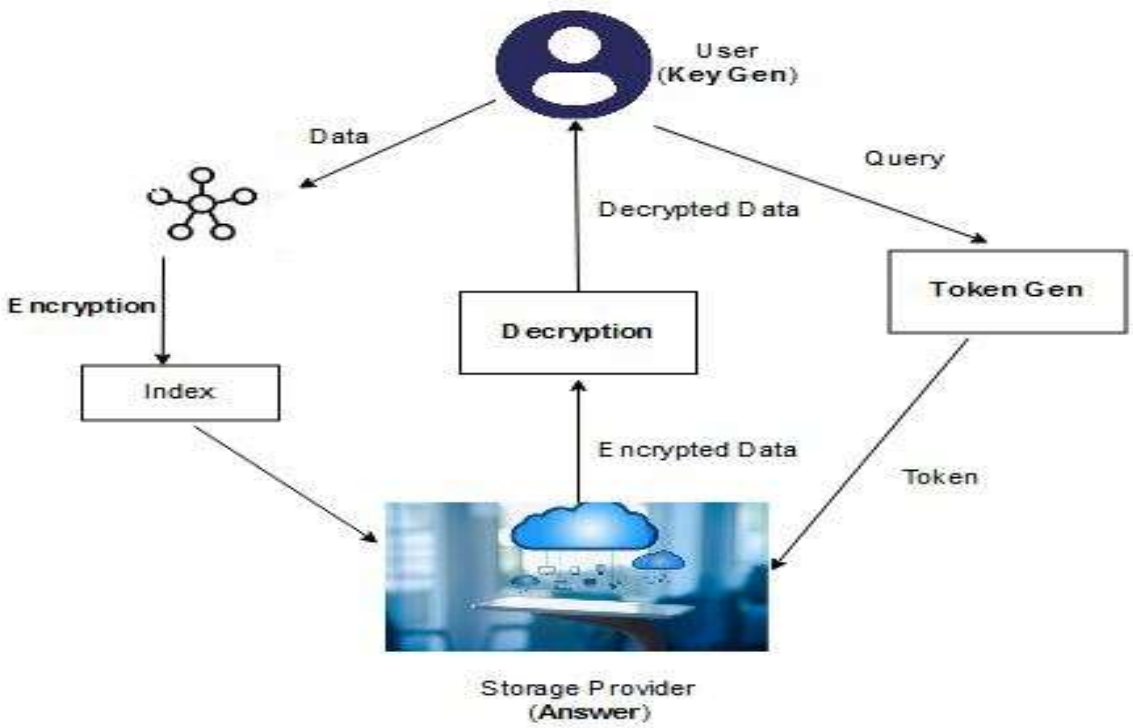
Cloud computing refers to the set of computing services like servers storage, software analysis, database networking and many more over internet. The offering of these computing services are known as cloud providers. Cloud Security or Cloud Computing Security consists of set of policies, technologies and controls deployed to secure or protect data,application. Data needs to be encrypted at all times with clearly defined roles. Cloud computing and storage provides users with capability to store and process the data in 3rd party data center. Security issues are faced by cloud providers and also by customers. However, the responsibility is shared and that their client's data and application are protected, while the users must take measure to fortify their application and use strong password and authentication measures.

Graph encryption based data outsourcing has become an important application used in cloud computing [3]. The data owners has no work to maintain the IT infrastructure and data management because data is encrypted in such a way there is no leakage in information. This is biggest challenge towards cloud computing. In traditional encryption techniques, outsourced data has no longer queryable which would severely impact on data usability[1] [6].

II. SYSTEM ARCHITECTURE

The user registers the details and then sign in for further process. User stores the encrypted data in cloud. For high security demands, data in encrypted using graph coordinates in graph encryption scheme. The important five algorithms are used in graph encryption scheme which are Encrypt algorithm, KeyGen algorithm, Token algorithm,Answer algorithm, Decrypt algorithm. Data is stored in graph structure and using encryptionalgorithm as result it produces index [1]. In this algorithm, index is formed based on all types of search queries. Four main indexes are used, firstly KeywordIndexGenis for encrypting keywords of the data file twice and secondly HopIndexGen is for identifying the nearest keywords for the users search keyword and next index NeighborIndexGen if two vertices containing same keywords then process of searching will be slow, to overcome this difficulties NeighborIndexGen is used and lastly LoopupIndexGen is normally for searching in which vertex the queried keyword in available. These indexes are combined to produce an index in Encrypt algorithm and it is stored in cloud.

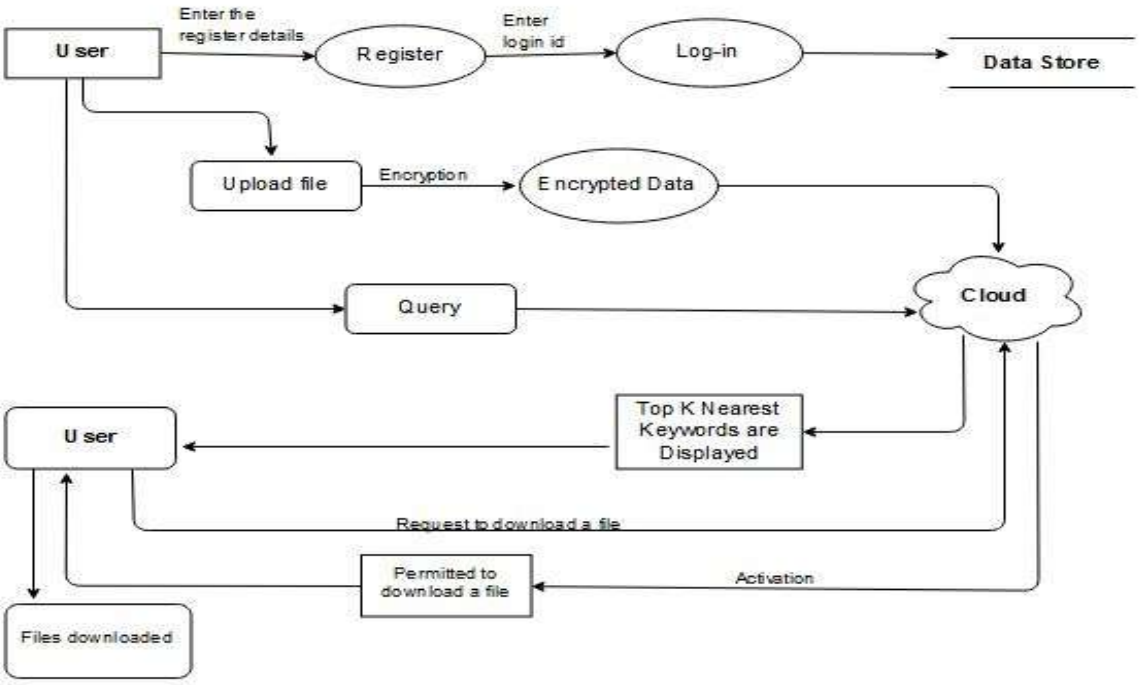
Now users can reuse the data anytime. While retrieving data user make search query in cloud. The keyword of the file is searched in the cloud. When queries are raised, it produces the token for each keyword using token algorithm. Now token is saved in cloud. Using answer algorithm, index and token is combined to form complete encrypted data. This encrypted data is decrypted using key which is send to unique id of user such as email id, phone number, etc. With the help of key data is decrypted using decryption algorithm.



III. BLOCK DIAGRAM

The user must fill the detailfor register process. It includes details like user name, email id, gender, date of birth, password, phone, address. Following that process, user login and upload the files to the cloud by selecting two coordinates for each file. Now when user need to retrieve the data. User again login into their account and in search box, user makes the query. As a result it displays the Top-K Nearest Keywords for the search query. Once nearest keywords are displayed user can select the particular file they want. When file is selected, token is generated to the cloud (Service Provider). i.e., token is the request for downloading the data files.

Now service provider activates the token request. Now user can download the files from the cloud. While uploading data files, two coordinates are selected by users are used to generated the key for decryption. This key is send to user's unique id such as email id. With the help of key files can be decrypted.



CONCLUSION AND FUTURE SCOPE

In this paper, we aresecuring our own data. We propose graph encryption method. In this approach encrypted data is stored in a graph structure. By using the graph encryption, application provides high security in cloud computing. Security is not only for third parties even for storage providers.Queries result as user friendly top-k nearest keywords. In future work, KNK complex queries on graph encryption scheme like classifications and clustering.

REFERENCES

[1] Chang Liu, Liehuang Zhu, Jinjun Chen, "Graph encryption for top-k nearest keyword search queries on cloud" in IEEE Trans., 2017.

[2D. Liu and S. Wang.Programmable order-preserving secure indexfor encrypted database query. In IEEE Cloud Computing (CLOUD),pages 02–509, 2012.

[3] D. X. Song, D. Wagner, and A. Perrig. Practical techniques forsearching on encrypted data. In IEEE Symposium on Security andPrivacy, SP'00, pages 44–55, 2000.

[4] R. Agarwal, P. Godfrey, and S. Har-Peled. Approximate distancequeries and compact routing in sparse graphs. In IEEE INFOCOM,pages 1754–1762, 2011.

[5] V. Chang, Y.-H. Kuo, and M. Ramachandran. Cloud computingadoption framework: A security framework for business clouds.Future Generation Computer Systems, 57:24–41, 2016..

[6]J. He, M. Dong, K. Ota, M. Fan, and G. Wang.Netseccc: A scalableand fault-tolerant architecture for cloud computing security. Peerto-Peer Networking and Applications, 9(1):67–81, 2016.

[7] L. Zhang, L. Wei, D. Huang, K. Zhang, M. Dong, and K. Ota.Medaps: secure multi-entities delegated authentication protocolsfor mobile cloud computing. Security and Communication Networks, 9(16):3777–3789, 2016.

[8] 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.

[9] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu,and M. Steiner. Dynamic searchable encryption in very largedatabases: Data structures and implementation. In NDSS, 2014.

[10] J. Cheng, A. W.-C. Fu, and J. Liu. K-isomorphism: privacy preservingnetwork publication against structural attacks. In ACMSIGMOD, pages 459–470, 2010.