Enhancing Security using Revocable Identity based Encryption Algorithm in Cloud Computing

Dr.A.Akila
Assistant Professor
Department of Computer science
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.
Tamilnadu. India.
akila.scs@velsuniv.ac.in

R.Padma
Assistant Professor,
Department of Computer Science
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.
Tamilnadu. India.
padma.scs@velsuniv.ac.in

S.Prasanna
PG Student
Department of Computer science
School of Computing Sciences
Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai.
Tamilnadu. India.
prasannavenkatesh51@gmail.com

Abstract-The area of trade and other sectors needs the encryption of information to ensure security of the information. The information stored in the cloud or edge requires encryption before sending to the cloud or edge. At most care has to be taken to encipher the information that are stored in a remote location. Many researchers has been carried out in the encrypted information such as keyword search etc. The research in the field of graph structured information lacks. This paper mainly focuses on analyzing the technique for graph secret writing which performs the complex graph question sort. The technique is named as K Nearest Keyword Technique (KNK). Many Index approach is used to store the data that gives the answer for the queries. The vertex identifiers, keywords and edge area units are encrypted using the proposed Revocable Identity based Encryption (RIBE) algorithm. The RIBE algorithm assures providing security to the non-public data.

Keywords-Cloud computing, KNK Graph Encryption, Security, Efficiency, Revocable Identity based Encryption

I. INTRODUCTION

Cloud and Edge based computing makes the data owners to outsource the data instead of maintaining the system infrastructure and data management. The real challenge with cloud computing is its security issues. As the storage of information from cloud is transferring towards edge computing which has severe data privacy issues as the privacy risks with edge is higher than cloud computing [1].

To have data privacy, the sender should encrypt data before sending the data. The traditional encryption technique does not support querying and leads to decrease on data usability. Many researches have been carried out to make the keyword search on encrypted text data possible. But performing the query process on encrypted graph structure data is a state of art complex problem.

II. LITERATURE SURVEY

A. Distance Queries and Compact Routing in Sparse Graphs

A graph could be represented using the distance query data structure and the shortest route among any two vertices could be computed using the distance query data structure. A space of Ω(n1+1/k) is required for storing 2k Ω1 paths of n nodes in any data structures. The dense graphs with average degree Ω (n1+k) requires this space of Ω(n1+1/k) which is the lower bound. To eliminate this lower bound barrier, Agarwal et al proposed a work [2] with more query time. In general, graphs needs O(n3/2) space for a 3 paths stretch. The proposed work by Agarwal requires only O(n3/2) space for 2 paths stretch while other data structures requires O(log n) space. The work supports the major category of simulations on graphs such as AS level Internet Graph.

B. Fast Exact Shortest-Path Distance Queries

To tackle with larger actual world graphs like social networks, communication networks, a work is proposed by Akiba et al [3]. The shortest path of these bulk graphs could be found using breadth first search which requires more time as the networks cloud have million nodes and billions of edges. To solve this problem of complexity, they proposed a work that uses some sample nodes. The distance between other nodes and sample nodes is calculated and it is used to solve the distance related queries.

Akiba et al proposed an approach which provides a solution to select the sample nodes that cover the various areas of the graph. The algorithm proposed shows high accuracy and uses the same computation time when compared to existing approaches.

C. Partitioned Multi-Indexing

The insects such as bees, ants segregate a chemical named pheromone to communicate with other bees and ants. An aggregation pheromone is a pheromone that makes use of the clumping and clustering characteristics of the species to make the species come closer. The proposed work by Goel et al is the aggregate pheromone clustering. The Ant element is made to move towards the data points and depending on density of the pheromone, the data are grouped into cluster. This clustering approach provided better result compared to existing clustering algorithms.

III. PROPOSED SYSTEM

A. Architecture of KNK Graph Encryption:

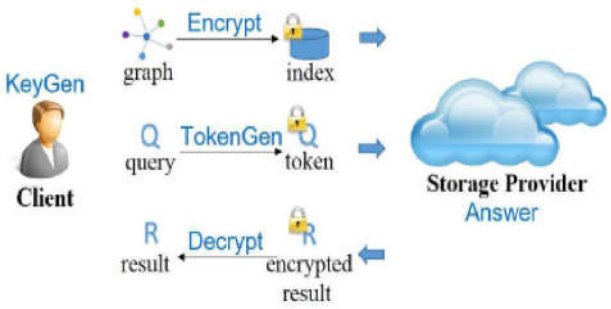

Fig 1: Architecture of kNK Graph Encryption

An interesting and challenging knk graph encryption scheme for construction could be designed other graph encryption schemas such as clustering &classification which more complex could be implemented to enhance the capability of proposed work. The KNK graph graph encryption is used for the graphical encryption.

B. Architecture of the Proposed Work – Text Encryption

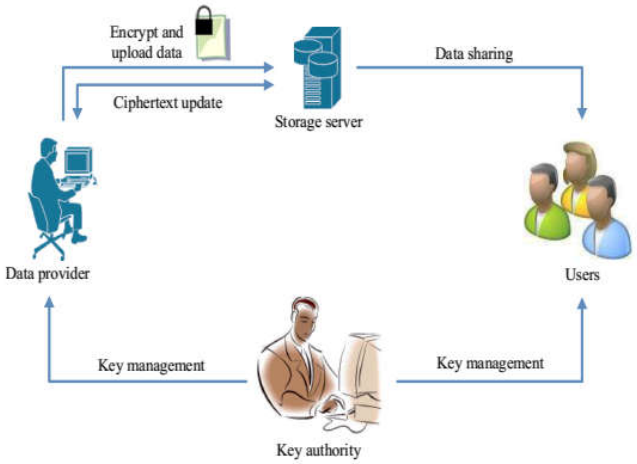

Fig 2: Architecture of the Proposed Work

1. Key Authority: Key authority provides intermediate connection between owner and user.
2. Data Provider: The data provider gives way to have services like data source connection, command execution and data fetch.
3. Data Sharing: The possibility of parallel change of same data in a distributed server environment should be prevented using some methodology.
4. Key Management: Key management provides intermediate connection user and data provider with keys.
5. User: The user can activate key authority and data provider.
6. Storage Server: The storage server acts as storage capacity of files into server storage system.
7. Encrypt& uploading data : Encrypt and uploading data can be uploaded by user with help of cipher text .

Data provider sends encrypt and upload data to storage server storage server sends to data sharing user can operates key authority the key authority sends user to key management and data provider

C. Modules of the Proposed Work

1. REGISTER & LOGIN: Before uploading the files in a cloud server, the user has to login. For the first time login, the user has to register himself and the details are stored in a database for future use. The username and password credentials are used to login by the user.
2. UPLOAD: This module deals with uploading the file by the user. The files uploaded are encrypted using data encryption standard algorithm. The uploaded files are stored in cloud server.
3. GRAPHICAL PASSWORD: In the proposed work, the password is a graphical password which uses the image as password. Human can remember images than text. The graphical password is more secures as it contains infinite search space [5].

4. REVOCABLE IDENTITY BASED ENCRYPTION

The text is encrypted using the Revocable Identity based Encryption. The revocable identity based encryption satisfies the security needs for data sharing. The duration of the transaction is added with the cipher text, so that when the cipher text is decrypted by the receiver within that specified duration.

a) Revocable Identity based Encryption Algorithm

RIBE-based data sharing system works as follows:
Step 1: The users who are going to share the data are first found by the data provider.
Step 2: Encryption of data is carried based on the user identity and the cipher text is uploaded to the cloud server.
Step 3: While downloading, the data is decrypted. The cloud server and unauthorized users are not allowed to decrypt the cipher text.
Step 4: If the user validity expires, the user cannot either upload or decrypt the data.

b) Advantages of Revocable Identity based Encryption Algorithm

- It gives the correct usage of RS-IDE algorithm and its security model.
- Both confidentiality and secrecy provided by the RS-IDE algorithm.
- It provides more security with respect to the ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption.
- The RS-IDE uses only public information to encrypt the data.

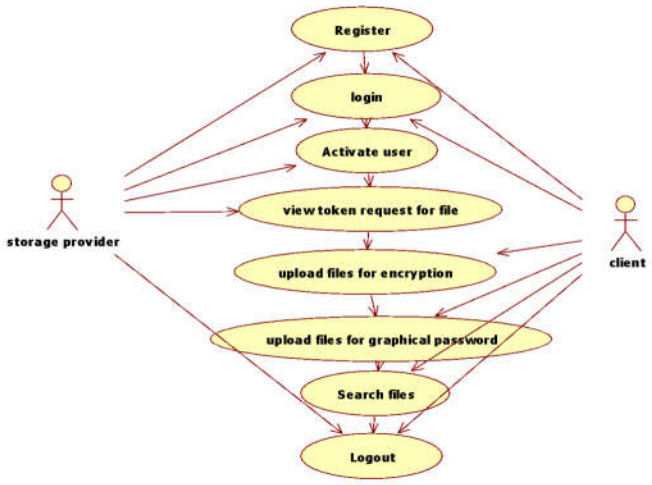

Fig 3:Flow Diagram of the Proposed work

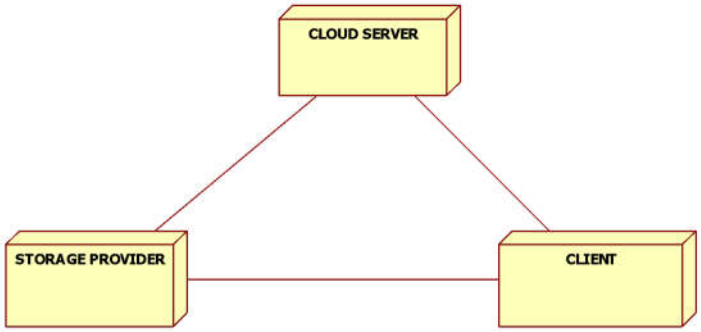

Fig 4: Deployment Diagram

IV. CONCLUSION

The KNK graph encryption with characteristics such as pseudo random function and symmetric key encryption is proposed. The proposed graph is used in a variety of areas like social networks, e amps, criminal analyses etc. The KNK graph encryprion have high security when compared to existing approaches. The RIBE algorithm encrypts the text with more accuracy..

REFERENCE

[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.