International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

A Survey on Implementing Graph Encryption for Top-k Nearest Keyword Search

Swati Shinde, Shweta Kotame, Nikita Dhokchaule, Pradnya Barve
Department of Information Technology, S.N.D college of Engineering and Research center, Savitribai Phule Pune University, Yeola, Nasik, India

ABSTRACT

Now a days the security demands of data outsourcing applications is increasing and it is becoming an important issue in sustainable smart cities. Client's data which is encrypted has been widely accepted by industry. As the clouds and edges are not far trusted encryption of data should be done at client side and then it should be outsource. Therefore, it is challenging issue that how to correctly encrypt the data so that encrypted and remotely stored data can be queried to get it back. We noticed that not so much people have worked on approaches for graph –structured data encryption and support for graph queries answering so it is still lacking in studies. In this paper, we investigate one graph encryption method called top-K Nearest Keyword(kNk) searches .it is an important graph query type, several indexes are design to store information which is necessary to answer queries and to maintain the privacy or security about the graph .It may be vertex identifiers, keywords and edges. Our graph encryption methods are secure or not is demonstrated by theoretical proofs and experiments which is done on real-world datasets.

Keywords: Graph Encryption, Clouds, Edges, Top-K Nearest Keyword Search

I. INTRODUCTION

Cloud computing and edge computing consist of different applications, data outsourcing is also important application of cloud computing. data outsourcing is nothing but storing client's data remotely on cloud and accessing it whenever required. While data is outsourced the security of data should be maintain so that client will store his/her data with trust, so encryption of data is done before it is outsourced. Data encryption is nothing but process of converting plain text data to cipher text data, this is done with the help of one secure key. But the traditional encryption methods does not support more data usability because such data is no longer queryable. Then also lots of work have been made for keyword search on encrypted textual data, but still various queries on encrypted graph structured data is challenging problem.

Top-k nearest keyword (kNk) search is taken into consideration because of its important applications in graph. kNk consist of a graph G = (V, E) where V is set of all vertices of graph (i.e. v ∈V) and E is set of all edges of graph. In this method each vertex labeled with range of keywords (w). An input given to the kNk search is (k, v, w), kNk search give result such that k vertices in graph which are labeled with w keyword and are nearest to vertex v.

In this paper we study, kNk search gives secure data outsourcing setting, i.e. how to properly encrypt graph and securely answer kNk search queries. It is noticed that while performing kNk queries on graph there was lots of information leakage from queries and graph also. So, for query we should at least able to hide content and identifiers of w and v respectively. And for graph we should able to hide all vertex identifiers. For example, in real life the vertex identifiers could be Email-Id, mobile number, Name, Address etc. To cover all above needs, the special encryption method for graphs should be designed.

By using the AES encryption method the information leakage due to graph can be avoided but it does not support the query on such graph, it encrypts whole graph. Whereas encrypting partial graph leeks too much

information and generates high risk in real world usage. That means if whole graph structured is leaked then it is easy to perform various attacks on such a graph. For example, vertex re-identification attacks. We are going to contribute following things: 1. On encrypted graph investigate kNk queries. 2. Defining a typical graph encryption scheme which will support kNk queries and its security model is offer. 3. Conducting performance evaluation of proposed graph encryption scheme on real-world graphs.

II. Literature Survey

D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searching on encrypted data. [1] Proposed first SSE scheme. Series of searchable symmetric encryption (SSE) works firstly addressed querying on encrypted and remotely stored data. This supports the keyword search on text data or documents. M. Chase and S. Kamara. [2] Structured encryption and controlled disclosure Chase and Kamara invented querying on structured data, because till the work was done on textual data only. They also proposed some structured encryption schemes. For example, matrix-structured encryption scheme supporting lookup queries, graph encryption scheme answering sub graph queries, graph encryption scheme supporting neighbor queries, adjacency queries etc.it is difficult and challenging issue to designing graph encryption method which will support higher-leveled query types such as keyword search. Pengtao Xie and Eric Xing. CryptGraph: Privacy Graph Analytics on encrypted Graph.[3] They are one who proposing to encrypt a graph with homomorphic encryption, which can protect all the structure information of a graph without losing the ability to perform graph analytics over it. C.R. Barde, Pooja Katkade, Deepali Shewale, Rohit Khatale. Secured multiple-keyword search over Encrypted Cloud Data [4]. In this paper, they propose the problem of Secured Multi-keyword Search (SMS) over encrypted cloud data (ECD), and construct a group of privacy policies for such a secure cloud data utilization system. They first proposed a basic Secured multi keyword ranked search scheme using secure inner product computation, and then improve it to meet different privacy requirements. The ranked result provides top k retrieval results. Babitha M.P, K.R. Ramesh Babu. Secure Cloud storage using AES encryption [5] this paper addresses different data security and privacy protection issues in cloud computing environment and propose a method for providing different security services like authentication, authorization and confidentiality along with monitoring in delay. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is encrypted using AES and then uploaded on cloud. They also used Short Message Service (SMS) alert mechanism for avoiding unauthorized access to user data.

III. Proposed System

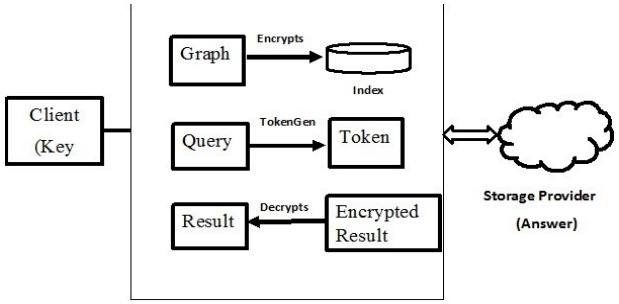

Figure 1. System Block Diagram

In this paper throughout we have used labeled graph. We define graph as G=(V,E) but in our paper we are using the keywords which are labeled to the vertices so, here graph can be defined as G=(V,W) where V is set or dictionary of identifiers of v's neighbor denoted as V[v], every vertex of graph has this kind of dictionary. Every w keyword labeled in the graph has dictionary (i.e. W). It is denoted as W[w].it stores identifiers of vertices which are labeled with w. The kNk queries should be answered on encrypted graph properly and for that purpose the graph should be correctly encrypted. Then and then the proper data outsourcing will take place, then client will able to store his data on cloud and access it whenever required. For focusing on kNk queries answering scheme, a graph encryption scheme consist of 5 algorithms such as 1.KeyGen i.e. key generation algorithm, 2. Encrypt for encryption, 3.TokenGen i.e. token generation algorithm 4.Answer 5.Decrypt for decryption.

Our outsourcing system involves client and storage provider. Client will own the graph say G which is to be outsourced, and storage provider will store encrypted form of G. Now client will able to fire kNk query on encrypted graph to access it again from storage provider and storage provider will answer client's kNk queries. The system contains 2 protocols

Setup protocol and Query protocol. In Setup protocol, client owns a graph and assigns the information in graph and then encrypt it with the help of graph encryption scheme, and outsource it to storage provider. And During Query protocol, client issues kNk query with the help of token which is also encrypted by token generation algorithm. The storage provider will return list of k graph vertices to the client. Fig 1describes the working of our system.

5.1 Algorithms Used:

1. K ← KeyGen (λ): is algorithm for secret key generation, it takes input as a security parameter λ and gives output a secret key K.
2. I ← Encrypt (K,G) : is algorithm used for encryption that takes input a secret key K and a graph G and it gives output secure index structure I.
3. T← TokenGen (K,k,v,w) : is the token generation algorithm that takes as input a secret key K, an integer k , a vertex identifier v and a keyword w and it gives output as a generated token T.
4. R ← Answer (I,T) : is the answer algorithm used at storage provider side to give answer to the client, it takes input as index I and a token T and outputs an encrypted result R to client side.
5. S ←Decrypt (K,R) : is the decryption algorithm that takes as input a secret key K and encrypted result R and outputs a set of k vertex identifiers S.

In above section we have not mentioned how to encrypt and decrypt graph data before outsourcing. The graph data is actually encrypted and decrypted independently using any symmetric-key generation algorithm. The symmetric-key algorithm uses same key at both sender and receiver side i.e. encryption and decryption both done with the help of same secret key.

IV. Advantages

1. Avoids information leakage which takes place in graph encryption.
2. Provides more security and efficiency to client's data as the graph itself is encrypted.
3. Encryption is done on client side before outsourcing of data, which make data more secure.
4. Innovated new graph encryption scheme.
5. Supports new graph query type.
6. Supports Top-k Nearest Keyword search on stored data.
7. Provides quick response to client's query.
8. Guarantee that private information about the graph such as vertex identifiers, keywords and edges (email, full names or phone numbers in real usage) are encrypted.

V. Applications

1. Can be used in social media sites to store user's data securely.
2. In government applications also used to store maps of villages etc.
3. It can be also used in industry area
4. Can be used in hospitals to store patient's data securely.

VI. Conclusion

Finally we can conclude that we did use of graph encryption. And we have presented the graph encryption scheme for kNk queries. Our graph encryption scheme makes use of some cryptographic primitives such as symmetric key encryption, rather than slow homomorphic encryption. The proposed encryption(graph) scheme is more user friendly with wide set of graph data based cloud computing and edge computing applications such as social networks, e-maps , government applications, criminal analysis, hospital databases, military applications etc.

Our scheme attains higher security level as compare to graph encryption approaches. In our system graph itself is encrypted and we do not make any assumption on attacks.

VII. REFERENCES

[1]. D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searching on encrypted data. In IEEE Symposium on Security and Privacy, SP'00, pages 44-55, 2000.

[2]. M. Chase and S. Kamara. Structured encryption and controlled disclosure. In ASIACRYPT, pages 577-594. Springer, 2010.

[3]. Pengtao Xie and Eric Xing. CryptGraph: Privacy Graph Analytics on encrypted Graph. School of Computer Science, Carnegie Mellon University Pittsburg.

[4]. C.R. Barde, Pooja Katkade, Deepali Shewale, Rohit Khatale. Secured multiple-keyword search over Encrypted Cloud Data. Department of computer, GESRHSCOE, Nasik, Maharashtra.
[5]. Babitha M.P, K.R. Ramesh Babu. Secure Cloud storage using AES encryption. Department of IT, Government Engineering College Idukki, Kerala.