International Journal of Engineering Research and Management (IJERM) – Volume-4, Issue-1, March2018

Cloud Security using Graph Encryption

Ms. A. S. Aher[1], Prof. D. S. Thosar[2], Prof. K. K. Patil[3]

[1]Lecturer, Department of Computer Technology,K. K. Wagh Women's Polytechnic,

[2]Assistant Professor,Department of computer Engineering, SVIT,Chincholi,Nashik.

[3]Assistant Professor,Department of Information Technology,PVG COE,Nashik

[1]aherashwini28@gmail.com

[2]devidas.svit@gmail.com

[3]kiran.patil@pvgcoenashik.org

Abstract *— In today's world security demands of data outsourcing applications in sustainable smart cities increases. Encrypting clients' data has been widely accepted by organization. Data encryptions should be done at the client side before contract out, because clouds and edges are not so much secure. So, how to properly encrypt data in a way that the encrypted and remotely stored data can still be queried has become a challenging issue. Though keyword searches over encrypted textual data have been extensively studied, approaches for encrypting graph-structured data with support for answering graph queries are still lacking in the literature. This paper illustrates graph encryption method. It is an important graph query type, named as top-k Nearest Keyword (kNK) searches. We design several indexes to store necessary information for answering queries and guarantee that private information about the graph such as vertex identifiers, keywords and edges are encrypted or excluded. Efficiency and security of graph encryption technique are revealing by theoretical proof. Also the experiments on real-world datasets use for security checking.*

Keywords — *Graph Encryption, Top-K Nearest Keyword Search, Searchable Encryption, Cloud Computing, Edge Computing.*

I. Introduction

Many real-world networks contain labels or textual contents on the nodes now days. On such networks, keyword search techniques on graphs have been used in a wide range of real-life applications in recent years. Given a undirected graph and a query request with a query node and a set of query keywords, a top- k nearest keyword (kNK) search finds k nodes which contain query keywords and are nearest to the query node. For example, Alice looks for k parks nearest to her home in road networks, where a location is labeled with "hospital", "school" or "park", etc., or Bob looks for k nearest friends with interests of hiking in a social network, where friends have personal information including name, skills and interests, etc.. For achieving great cost savings, more data owners are motivated to outsource their graphs to the cloud for storage, management and retrieval.

II. Literature Survey

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 lot efforts have been made to enable keyword search on encrypted textual, how to perform various queries on encrypted graph structured data is still a challenging problem.

III. PROPOSED SYSTEM

Top-k nearest keyword (kNK) search has been addressed recently due to its important applications in graphs. kNK search involves a graph G = (V;E) in which each vertex v 2 V is labeled with a range of keywords. On input (k; v;w), kNK search returns k vertices in the graph which is labeled with keyword w and are nearest to vertex

For example, in a social network, kNK search can answer such as "k = 5 most closely related person to v = John with interest keyword = basketball". In this paper, we study k-NK search in secure data outsourcing setting, i.e., how to encrypt a graph properly and answer kNK search queries in a secure manner. When performing kNK queries on an encrypted graph, privacy information would be leaked from both the graph and the queries. For the graph, we should at least hide all vertex identifiers, as which might be email addresses, full names or phone numbers in real usage. For a query (k; v; w), we should at least hide the identifier of v and the content of w. To attain all above requirements, the

encryption method for the graph should be specially designed. Though using traditional cryptographic encryption tools such as AES to encrypt the entire graph can avoid any information leakage, the resultant encrypted graph seems impossible to be queried. Whereas we partially encrypt a graph such as only encrypting vertex identifiers and keywords, the resultant encrypted graph leaks too much information which would result in high risks in real usage. For example, the graph structure is completely leaked so that an adversary is easy to perform various attacks such as vertex re-identification attacks.

A. System Architecture

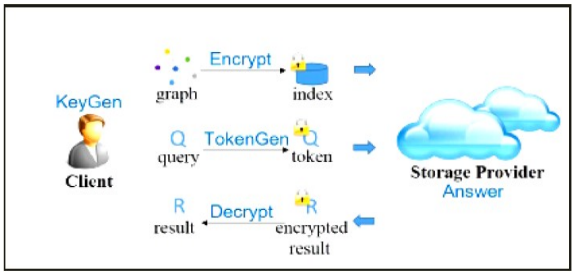

Fig.1 System Architecture of the Cloud Security Using Graph Encryption

Above diagram show the system of the Cloud Security Using Graph Encryption. In which when the client/user want to put the data on cloud have to first encrypt the data on the users side using graph encryption and then put on the cloud. And while accessing the data user have to decrypt it. And when other users want to access that data have to send the request for that in the form of token.

B. System Features

This system illustrates organizing the functional requirements for the Cloud Security Using Graph Encryption. Following are some features of the Cloud Security Using Graph Encryption: -

- Platform independent
- No centralized Servers required.
- Integrity, security for data files.
- Conversion of encrypted files into CSV conversion so that it will easy to provide security.
- Reduced hardware requirements
- Expense also get reduced
- Easy, fast and reliable system
- One system approach

C. Advantages

This system provides high availability & support to share data on cloud. Protection against unauthorized users is provided using graph encryption. More security & flexibility provided when data is share on cloud.

D. Limitations

This system provides high security to user for sharing data globally on a cloud. But when user want to share data it must require internet connection and the file or data is in encrypted format.

IV. Conclusions

This paper try out to provide security to the data on cloud both on client & server side.Proposed graph encryption scheme is user friendly environment. Compare to graph anonymization approaches from database community, this scheme attains higher security level as the graph itself is encrypted and It do not make any assumptions on the types of attacks

Acknowledgment

It is a great pleasure to acknowledge those who extended their support, and contributed time and psychic energy for the completion of this paper work. I am thankful to the all staff members of Computer Engineering Department and Librarian, SVIT, Chincholi, Nashik. Also I would like to thank my colleagues and friends and family members who helped me directly and indirectly to complete this work.

References (Size 10 & Bold)

[1] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou, Privacy Preserving Multi-keyword Ranked Search over Encrypted Cloud Data, The 30th IEEE Conference on Computer Communications (INFO COM'11), Shanghai, China, April 10-15, 2011.

[2] Haichuan Shang Ying Zhang Xuemin Lin, Jeffrey Xu Yu, Taming Verification Hardness: An Efficient Algorithm for Testing Subgraph Isomorphism, PVLDB '08, August 23-28, pp 364-375, New Zealand, 2008.

[3] Ning Cao, Zhenyu Yang, Cong Wang, Kui Ren, and Wenjing Lou, Privacy-preserving Query over Encrypted Graph-Structured Data in Cloud Computing,IEEE ICDCS2011, Minnesapolis, MN, Jun. 20-24, 2011

[4] Tero Harju, Lecture Notes on Graph Theory, Department of Mathemat ics University of Turku, Finland, 2011.

[5] Xifeng Yany, Philip S. Yuz, Jiawei Hany, Graph Indexing: A Frequent Structure-based Approach, SIGMOD-2004, June 13-18, Paris, France, 2004.

[6] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou,Attribute Based Data Sharing with Attribute Revocation, The 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'10), Beijing, China, April 13-16, 2010.

[7] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[8] J R Winkler, Securing the Cloud: Cloud Computing Security Techniques and Tactics, Elsvier Inc., USA, 2011.

[9] Cong Wang, Bingsheng Zhang, Kui Ren, and Janet M. Roveda, *Privacy Assured Outsourcing of Image Reconstruction Service in Cloud*, in IEEE Transaction on Emerging Topics in Computing, vol. (1):1, pp 166-177, June 2013,

[10] Mi Wen, Rongxing Lu, Kuan Zhang, Jinsheng Lei, Xiaohui, and Xuemin Shen, *PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid*, IEEE Transactions on Emerging Topics in Computing, vol (1):1, pp 178-191, June 2013.

[11] Wenjun Lu, Avinash L Varna and Min Wu, Confidentiality-Preserving Image Search: A Comparative Study Between Homomorphic Encryption and Distance Preserving Randomization, In IEEE Transactions on Content Mining, Vol. 2, March2014.

[12] D Song, D Wagner and A Perrig, *Practical Search Techniques for Searches in Encrypted Data,* In IEEE Proceeding of Symp. Res. Sec. Privacy, pp. 44-55, 2000.

[13] A Swaminathan, Y Mao, G M Su, H Gou and A L Varna, *Confiden tiality Preserving Rank Ordered Search*, in Proceeding ACM Workshop Storage Security Survivability, pp 7-12, 2007.

[14] R Brinkman, L Feng, J Doumen, P H Hartel and W Jonker, *Efficient Tree Search in Encrypted Data,* Infirmation System Security, June, 2004.

[15] Jin Li, at el., Enabling Efficient Fuzzy Keyword Search over Encrypted Data in Cloud Computing, 2011.

[16] E Mykletun and G Tsudik, Incorporating a secure coprocessor in the Database as a Service Model, In International Conference on IWIA,2005.