A NEW SECURE QUERY PROCESSING FRAMEWORK FOR LOCATION BASED SERVICES FROM THE WEB CLOUD

R. Lavanya., MCA., M.Phil., ME., Assistant Professor, Department of Computer Science,
Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.
K.P. Dharani, BSc (CS)., M.Sc (CS)., Department of Computer Science,
Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore.

ABSTRACT

Location Based Services (LBS) enables the user to access the information that is relevant to their location and point of Interest. Many existing approaches fail in applying the secure query processing framework for the sensitive data with up to date information. Information is the entity with large geo-tagged data composed by data owner. But typical data owners do not have the technical means to support processing queries on a large scale, so they outsource data storage and querying to a cloud service provider. Many such cloud providers exist who offer powerful storage and computational infrastructures at low cost. However, cloud providers are not fully trusted, and typically behave in an honest but curious. In this framework, we propose a query processing technique utilizing the kNN (Nearest Neighbour) algorithm against the Point of interest as user request to the cloud Service provider (broker), where broker computes the data owner's information to yield the high relevant data as retrieved information. To secure the data, we establish a Mutableness Order Preserving Encoding to protect user queries and point of interest data. The performance evaluation of the proposed hybrid methods which can be used to provide the optimized solutions which is used to combine many queries and process them and also yields good results in terms of decreased computational speed and less memory utilization against the state of approaches. It is important to note from the previous studies that the spatial queries which has the process of the nearest neighbour, range, skyline or keyword queries. It is also provided that there is no framework that can be processing all the queries in using the single entity so, it is notes that privacy based optimized query processing framework is lacking in the previous studies.

Index Terms: - Voronoi Diagrams, Delaunay tessellation, Spatial Database and LBS.

INTRODUCTION

Data mining means collecting, processing, storing and analyzing data in order to discover new information from it in the secured manner. Data mining depends on effective data collection and warehousing as well as computer processing. On the other hand cloud computing refers to a variety of services available over the Internet that delivers compute functionality on the service provider's infrastructure. Its environment (infrastructure) may actually be hosted on either a grid or utility computing environment, but that doesn't matter to a service user. Location Based Services provide the infrastructure of Data as a Service (DaaS) concept. It includes the process of finding the related locations to the required point of interest of the user. Key Management rises in the Private information retrieval Scheme and order preserving scheme.

Due to the specificity of such data, collecting and maintaining such information is an expensive process. B-Tree uses the more computation time for the retrieval of information which cannot be used for the larger datasets.

RELATED WORK

kNN Queries in Euclidean Space, kNN Queries in Spatial Networks and Single-source Skyline query in Euclidean space are mainly used which is provided in the previous studies [4][5]. Best Fit Network expansion is introduced for network distance calculations with customized encryption scheme using kNN query processing [2]. For travelling and tourism datasets have also been provided [6]. All of the above studies will consider a network distance as static where in real fast world shortest path computation depends on query processing time from one node to another [1]. All these above mentioned studies can be provided using the optimal solutions after the computations.

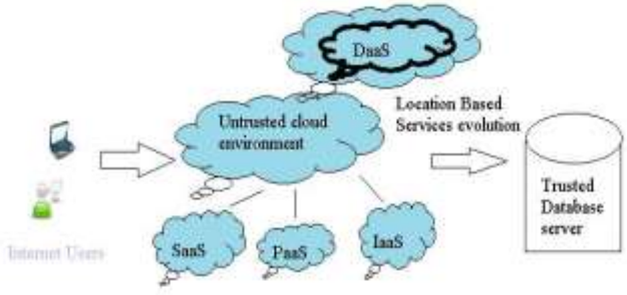
PROPOSED SYSTEM

We propose a query processing technique utilizing the K-NN (Nearest Neighbour) algorithm against the Point of interest as user request to the cloud Service provider (broker), where broker computes the data owners information’s to yield the high relevant data as retrieved information. To secure the data, we establish a mutable order preserving encoding to protect user queries and point of interest data.

Significance

- False positive rate is low in large sparse data extraction
- Precision of the results i s high
- Response time is low for retrieving even the distance data point through Euclidean distance calculation
- For Communication and memory utilization is low in Mutableness Order Preserving Encryption model

SYSTEM ARCHITECTURE


DaaS
Untrusted cloud environment
Location Based Services evolution
Trusted Database server
Internet Users
SaaS
PaaS
IaaS

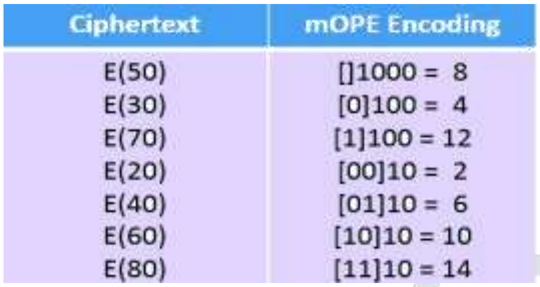
The system consists of the (i) client, (ii) untrusted cloud service provider, (iii) trusted data owner. The trusted data owner which has the valuable dataset with n 2-D points of interest, but it does not have a necessary infrastructure to maintain the datasets while large number of clients are using incrementally. So, the data owner will be having the encrypted format of the data about the user and it will be outsourced to the cloud provider. The dataset is a valuable resource of many users, so it has to be provided in the encrypted format to prevent from malfunctioning of any cloud service providers (i.e., the third party servers).

The client will be sending the query in the form of encrypted texts in the sense only the point of interest and the valuable data will be provided in the encrypted format so that the time to retrieve the information can be minimized. This encrypted format is provide along with those additional data structures (i.e., Voronoi Diagram, Delaunay tessellations) which is needed for the query processing and to indentify the shortest path between the point of interests. As the server receives the requests of the kNN from many clients, the server processes the requests and provides the results. Though the cloud service provider typically processes the request there will be a powerful computation of resources, this is provided because of the significant overheads that can be formed due to the encrypted data. Therefore, it is significant to incur the computation in the cloud service provider which works on the encrypted texts which has to minimize the overheads for processing efficiently. The client will be having the query point Q and then it finds the nearest neighbors. Then the client sends the encrypted cipher texts of the location based point to the server, and it receives along with the k Nearest Neighbors as a result.

APPLICATIONS

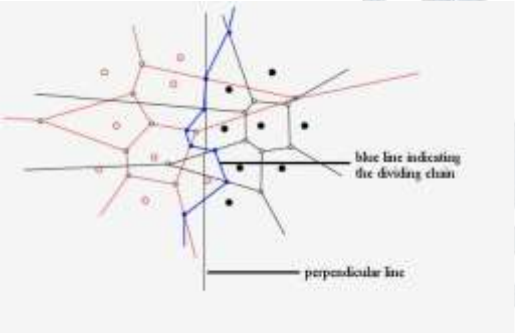
This type of kNN query processing is used in many fields which includes the Navigation which can be interpreted in any sector easily, it is also used in preserving of our datum from the third party sever and now in future its mainly going to be used in the car navigations which is used to find the shortest path very accurately without any delay in the processing time. It has widespread use in the Computational Geometry, City Planning, Computer Graphics, Epidemiology, Geophysics and Meteorology, also have central idea in TV series Numbers .

K-NEAREST NEIGHBOUR A LGORITHM FOR QUERY PROCESSING USING VORONOI DIAGRAM



Ciphertext	mOPE Encoding
E(50)	[]1000 = 8
E(30)	[0]100 = 4
E(70)	[1]100 = 12
E(20)	[00]10 = 2
E(40)	[01]10 = 6
E(60)	[10]10 = 10
E(80)	[11]10 = 14

CENTROID COMPUTATION: This is mainly done using the voronoi diagrams. The query point Q can be computed exactly by finding the centroid for the specified cell. (For Example, f=max is the center of the small circle containing the query point Q), it matches only with those centroid points and then it finds the path. Secondly, it can be computed in such a way that a perpendicular line will be drawn to that centroid and then it can also be further split to process the cells separately without any overheads which can be explained in the further diagram.



METHODOLOGY

- kNN queries on encrypted data requires complex operations, but at the core of these operations sits a relatively simple scheme called **Mutableness Order Preserving Encryption**. It allows secure evaluation of range queries, and is the only provably secure order preserving encoding system (OPES) that is known to date [8].

Our method employs both mutableness order preserving encryption and conventional symmetric encryption (AES), to avoid confusion we will further refer to mOPE operations on plaintext/cipher texts as encoding and deco ding, whereas AES operations are denoted encryption/decryption.

The mutableness order preserving encryption scheme in a client-server setting works as: the client has the secret key of a symmetric cryptographic scheme, e.g., AES, and wants to store the dataset of cipher texts at the server in increasing order of corresponding plaintexts. The client engages with the server in a protocol that builds a R-tree at the server. The server only sees the AES cipher texts, but is guided by the client in building the tree structure. The algorithm starts with the client string the first value, which becomes the Tree root. Every new value stored at the serve r is accompanied by an insertion in the R-tree.

The server maintains a mutableness order preserving encryption table with the mapping from cipher texts to encodings, for a tree with four levels (four -bit encoding). Clearly, mutableness order preserving encryption is an order preserving encoding, and it can be used to answer securely range queries without need to change to plain texts.

OPTIMIZATIONS

As in this system mod el the processing of the data in the encrypted format and this has become the reason for the expensive in the processing time. So, it has been the well-known fact that when the data are being provided in the encrypted format it will be expensive and also due t he computation time the overheads will be maximized than the before Plain texts computations. Thus, it is necessary to Provide the optimizations which as the aim at reducing the computation cost.

CONCLUSION & FUTURE WORK

The main performance metrics used to evaluate the proposed techniques are query response time and communication cost. VD-kNN provides exact results, but its performance overhead may be high. Tessellation kNN only offers approximate NN results, but with better performance. In addition, the accuracy of Tessellation kNN is very close to that of the exact method used. Overall, VD-1NN is considerably costlier than Tessellation *k*NN. It can be enhanced using the SKYLINE Queries which can be used to identify the further processing of the moving objects while performing navigation for the accurate results.

REFERNCES

[1] Bellare.M, Desai.A, Pointcheval.D , and Rogaway.P , “Relations among notions of security for public-key encryption schemes,” n Proc. Crypto ’98, Krawczyk.H Ed. Springer-Verlag, LNCS

[2] ‘Bin Yao’, Department of Computer Science and Engineering, Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong University, ‘ Feifei Li’ , China School of Computing, University of Utah School of Computer Engineering, ‘Xiaokui Xia’ , Nanyang Technological University, Singapore, “Secure Nearest Neighbor Revisited” , ICDE’13

[3] Huiqi Xu, Shumin Guo, and Keke Chen, “Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation”, TKDE’12

[4] Mehdi Sharifzadeh, Google and Cyrus Shahabi, University of Southern California in September 2010, “VoR-Tree: Rtrees with voronoi diagrams for efficient processing ofspatial nearest neighbor queries”, Vol. 3, No. 1

[5] Priya Iyer.K.B et al, “Privacy aware spatial queries” / Indian Journal of Computer Science and Engineering (IJCSE) ISSN : 0976-5166 Vol. 3 No.4 Aug-Sep 2012

[6] Qi Lui, Enhong chen, Senior Member, IEEE, Hui Xiong, Senior Member, IEEE, Yong Ge, Zhongmou Li, and Xiang Wu, “A Cocktail Approach for Travel Package Recommendation” , VOL. 26, NO. 2, FEBRUARY 2014

[7] Seung-HyuSeo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE in September 2014, “An Efficient Certificate less Encryption for Secure Data Sharing in Public Clouds” Vol. 26, No. 9

[8] C.B.Sivaparthipan, S.Raja Ranganathan, Prabakar.D, Dr. T.Kalaikumaran, “INCREASING THE ACCESSIBILITY OF DATA SETS BY USING DISTRIBUTED ALGORITHM IN DATA MINING”, IJRCAR,INDIA

[9] Sunoh Choi, Gabriel Ghinita, Hyo Sang Lim and Elisa Bertino, “Secure kNN query processing in unstructed cloud environment” , VOL.26, JUNE 2014

[10] Wong.W.K , David W. Cheung , Ben Kao, Nikos Mamoulis, “Secure kNN Computation on Encrypted Databases” SIGMOD’09, June 29–July 2, 2009, Providence, Rhode Island, USA

[11] Zohreh Alavi, Lu Zhou, James Powers, Keke Chen Data Intensive Analysis and Computing (DIAC) Lab, Kno.esis Center Department of Computer Science and Engineering Wright State University, Dayton, Ohio 45435, USA

[12] K.Vengatesan, Mahajan S. B., Sanjeevikumar P., Kulkarni R. M., Sana Moin Submitted a paper on “Similarity Measurement of Gene Using Arc Tan Function in Gene Ontology” ,Advances in Systems, Control and Automation, Lecture Notes in Electrical Engineering 443, DOI 10.1007/978-981-10-4765-7_83, Chapter No.: 83

[13] K.Vengatesan, Mahajan S. B, Sanjeevikumar P., Mangrule Rupali A, Kala V, Pragadeeswaran S, Submitted a paper on “Performance analysis of Gene Expression data using Mann-Whitney U Test” , Advances in Systems, Control and Automation, Lecture Notes in Electrical Engineering 442, DOI 10.1007/978-981-10-4762-6_67 , Chapter No.: 67 (Springer Publication Scopus Index Accepted).