Volume 2, Issue 2 February 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal Of Science, Engineering and Information Technology

NAIRJC JOURNAL PUBLICATION
North Asian International Research Journal Consortium
Nairjc....
North Asian International Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

SECURE QUERY PROCESSING IN UNTRUSTED CLOUD ENVIRONMENTS USING kNN

SNEHAL J. AVACHAT, MOHINI D. MANE, NUTAN N.WISAWE, DHANASHREE D.TIKONE,

PROF. PRAMOD PATIL*

*Department of Inforamtion Technology, NMVPM’s, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Pune. 410507

Abstract—.*Cell phones with geo-positioning capabilities register users to access information that is applicable to their present and current location. Clients are occupied with questioning about purposes of interest (POI) in their physical vicinity, for example, eateries, bistros, progressing occasions, and so forth. Elements worked in different territories of interest (e.g., certain specialty bearings in expressions, excitement, travel) assemble a lot of geo-labeled information that engage subscribed clients. Such information may be touchy because of their substance. Moreover, staying up with the latest and significant to the clients is not a simple errand so the proprietors of such datasets will make the information available just to paying clients. Clients send their present area as the inquiry parameter, and wish to get as result the closest POIs, i.e., closest neighbors (NNs).Data is stored with a third party in cloud environments and query processing is also done by third party to reduce the amount to maintain the system Our strategies depend on variable request protecting encoding (mOPE), the main secure request saving encryption technique known not. We additionally give execution enhancements to diminish the computational expense innate to preparing on encoded information, and we consider the instance of incrementally upgrading datasets. We introduce a broad execution evaluation of our strategies to show their practicality by and by.*

***Keywords—* location privacy, mutable order preserving encoding, database outsourcing, spatial databases**

I. INTRODUCTION (*HEADING 1*)

The rise of cell phones with quick Internet availability and geo-situating capacities has prompted an insurgency in redid area based administrations (LBS), where clients are empowered to get to data about purposes of interest (POI) that are pertinent to their intrigues and are likewise near their land organizes. Presumably the most vital sort of questions that include area characteristics is spoken to by closest neighbor (NN) inquiries, where a client needs to recover the k POIs (e.g., eateries, galleries, corner stores) that are closest to the client’s present area (kNN). An inconceivable measure of exploration concentrated on performing such questions effectively, ordinarily utilizing some kind of spatial indexing to lessen the computational overhead .The issue of security for clients' areas has likewise increased critical consideration previously. Note that, all together for the NNs to be resolved; clients need to send their directions to the LBS. Then again, clients may be hesitant to uncover their organizes if the LBS may gather client area follows and utilize them for different purposes, for example, profiling, spontaneous ads, and so on. To address the client protection needs, several conventions have been recommended that withhold, either mostly or totally, the clients' area data from the LBS. Case in point, the work in replaces areas with bigger shrouding districts that are intended to avert divulgence of definite client whereabouts. By and by, the LBS can at present get touchy data from the shrouded areas so a different line of examination that uses cryptographic quality assurance was begun in and proceeded in. The primary thought is to augment existing Private Information Retrieval (PIR) conventions for paired sets to the spatial space, and to permit the LBS to give back the NN to clients without realizing any data about clients' areas. This system fills its need well, yet it expects that the genuine information focuses (i.e., the purposes of hobby) are accessible in plaintext to the LBS. This model is suitable for general-interest applications, for example, Google Maps, where the historic points on the guide speak to open data; however can't deal with situations where the information focuses must be shielded from the LBS itself.

II. EXISTING METHODLOGY

Existing system vast amount of research focused on performing such queries efficiently, typically using some sort of spatial indexing to reduce the computational overhead. The issue of privacy for users' locations has also gained significant attention in the past. Note that, in order for the NNs to be determined, users need to send their coordinates to the LBS. However, users may be reluctant to disclose their Started in and continued in. The main idea is to extend existing Private Information Retrieval (PIR) proto-cols for binary sets to the spatial domain, and to allow the LBS to return the NN to users without learning any in-formation about users' locations.

III. SCOPE

Due to the specificity of such data, collecting and maintaining such information is an expensive process, and furthermore, some of the data may be sensitive in nature. For instance, certain activist groups may not want to release their events to the general public, due to concerns that big corporations or oppressive governments may intervene and compromise their activities. Similarly, some groups may prefer to keep their geo-tagged datasets confidential, and only accessible to trusted subscribed users, for the fear of backlash from more conservative population groups. It is therefore important to protect the data from the cloud service provider. In addition, due to financial considerations on behalf of the data owner, subscribing users will be billed for the service based on a pay per result model. For instance, a subscriber who asks for kNN results will pay for k items, and should not receive more than k results. Hence, approximate querying methods with low precision, such as existing techniques that return many false positives in addition to the actual results are not desirable.

IV. MOTIVATION

To provide the user location information in encrypted format to the cloud server. To receive the data sets of point of interest from the data owner in encrypted format. To provides the point of interests of user query from the k Nearest Neighbor to the client.

V. ISSUES IN EXISTING SYSTEM

Existing system vast amount of research focused on performing such queries efficiently, typically using some sort of spatial indexing to reduce the computational overhead [1]. The issue of privacy for user's locations has also gained significant attention in the past. Note that, in order for the NNs to be determined, users need to send their coordinates to the LBS. However, users may be reluctant to disclose their Started in [7] and continued in [8, 9]. The main idea is to extend existing Private Information Retrieval (PIR) protocols for binary sets to the spatial domain, and to allow the LBS to return the NN to users without learning any in-formation about user's locations.

VI. PROPOSED SYSTEM

We propose the VD-*k*NN method for secure NN queries which works by processing encrypted key. The method returns exact results, but it is expensive for *k*>1, and may impose a heavy load on the data owner. To address the limitations of VD-*k*NN, we introduce T *k*NN, a method that works by processing encrypted key, supports any value of *k* and decreases the load at the data owner. T *k*NN provides exact query results for *k*=1, but when *k*>1 the results it returns are only approximate. However, we show that in practice the accuracy is high. Encrypted key that allows us to deal efficiently, in an incremental manner, with changing datasets. We propose performance optimizations based on spatial indexing and parallel computation to decrease the computational overhead of the proposed techniques. Finally, we present an extensive experimental evaluation of the proposed techniques and their optimizations, which shows that the proposed methods scale well for large datasets, and clearly outperform competitors.

VII. RELATED WORK

Secure location data is an important problem in the scenario of outsourced search services, but in a variety of other settings as well. For illustration, two approaches for location secure have been considered in the context of personal queries to location- based services (LBS). The objective here is to allow a querying user to retrieve her nearest neighbor among a set of public points of interest without revealing her location to the LBS. The _rst approach is to use cloaking regions (CRs) [3],[4]. The CR based solutions implement the spatial k-anonymity model and assume a three- tier architecture where a trusted strong sits between users and the LBS server and generates rectangular area that contain at least k user locations. This method is fast, but not secure in the case of outliers. The second method uses private information retrieval (PIR) protocols [5]. PIR protocols allocate users to retrieve an object X from a set X = fX1;X2; :::;Xng stored by a server, without the server learning the value of i. In [5] describe an PIR protocol for binary data to the LBS domain and proposes approximate and exact nearest neighbor protocols. The latter approach is secure, but it is expensive. The use of Delaunay triangulations and Voronoi diagram are investigate to solve the problem of secure Knn queries[1],[5]. The elements of Voronoi diagram is present to the cloud provider in plaintext and processing on cipher texts.

VIII. METHODOLOGY

To support secure kNN queries, where kis fixed for all querying users, we could extend the VD-1NN method from by generating order-k Voronoi diagrams. However, this method, which we call VD-kNN, has several serious drawbacks: (1) The complexity of generating order-k Voronoi dia-gramsis either (k nlog n) or (k (n-k)logn+nlogn), depending on the approach used. This is significantly higher than O (nlog n) for order-1 Voronoi diagrams. (2) The number of Voronoi cells in an order k Voronoidiagram is O (k(n-k)), or roughly kn when k¡¡n. That leads to high data encryption over head at the data owner, as well as prohibitively high query processing time at the server (a k-fold increase compared to VD-1NN). Motivated by these limitations of VD-kNN, we first intro-duce a secure distance comparison method (SDCM). Next, in we devise Basic kNN (BkNN), a protocol that uses SDC Misguiding block, and answers Knn queries using repetitive comparisons among pairs of data points. BkNN is just an auxiliary scheme, very expensive in itself, but it represents the starting point for Triangulation kNN (TkNN), presented. TkNN builds on the BkNN concept and returns exact results for k=1. For k¿1, it is an approxima-tive method that provides high-precision kNN results with significantly lower costs.

IX. SYSTEM ARCHITECTURE

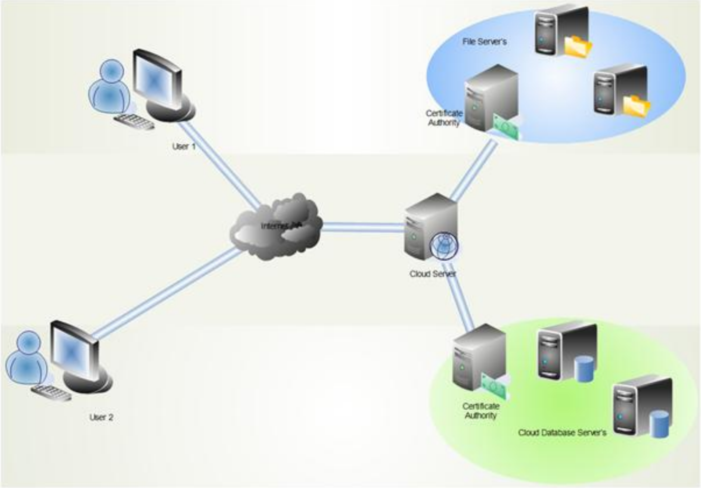

Figure 1: General Model for query processing in Cloud

X. ALGORITHM / PROTOCOL / MATHEMATICAL INDUCTION / METHODS USED

- Index Tree-based Search Algorithm: To Search the file in tree structure and also upload the files in tree.
- Improved method combining with KNN algorithm is higher than the original method combining with KNN algorithm
- Algorithm used to File Upload & Download at nearest neighbour nodes.
- RNM keys used CryptoSys API.
- Random Key Algorithm used to Security Purpose.

ACKNOWLEGDEMENT

We would like to express our gratitude to all those who helped us to complete this work. We want to thank our guide Prof. Pramodkumar Patil for his continuous help and generous assistance. He helped in a broad range of issues from giving us direction, helping to find the solutions, outlining the requirements. We would like to thank our colleagues who helped us time to time from preparing report and giving good suggestions.

CONCLUSION

We proposed two plans to backing secure k closest neighbor question handling: VDkNN which depends on Voronoi outlines, and TkNN which depends on Delaunay triangulations. They both use alterable order preserving encoding (mOPE) as building piece. VD-kNN gives accurate results, yet its execution overhead may be high. TkNN just offers rough NN results, yet with better execution. Likewise, the exactness of TkNN is near that of the accurate technique. In future work, we plan to research more mind boggling secure assessment capacities on iphertexts, for example horizon inquiries. We will likewise look into formal security insurance ensures against the customer, to keep it from learning something besides the got k question results.

REFERENCES

- Mark de Berg et.al. Computational Geometry, Springer.
- W.K. Wong, David W. Cheung, Ben Kao, and Nikos Figure 8-3. Data Encryption Time IEEE TRANSACTIONS ON KNOWLEDGE DTA ENGINEERING, VOL.26, JUNE, 2014 Mamoulis, Secure kNN Computation on Encrypted Databases, SIGMOD09
- Haibo Hu, Jianliang Xu, Chushi Ren, and Byron Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism, ICDE11.
- Huiqi Xu, Shumin Guo, and Keke Chen, Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation, TKDE12.
- BinYao, Feifei Li, and Xiaokui Xiao, Secure Nearest Neighbor Revisited, ICDE13.
- Raluca Ada Popa, Frank H. Li, and Nickolai Zeldovich, An Ideal-Security Protocol for Order-Preserving Encoding, IEEE S&P13.
- Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and Kian-Lee Tan, Private Queries in Location Based Services: Anonymizers are not Necessary, SIGMOD 08.
- Gabriel Ghinita, Panos Kalnis, Murat Kantarcioglu, and Elisa Bertino, A Hybrid Technique for Private Location- Based Queries with Database Protection, SSTD09
- Gabriel Ghinita, Panos Kalnis, Murat Kantarcioglu, and Elisa Bertino, Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection, Geoinformatica11

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com