International Journal of Engineering & Technology, 7 (3.34) (2018) 213-216

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Knn Search with Location and Query Solitude Using Bit Exchanging Method

[1]K. Suja, [2] Dr. A. Rengarajan

[1] Ph.D Scholar, Department of Computer Science & Engineering St Peter's University, Chennai, India
[2] Professor, Department of Computer Science and Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India

Abstract

In recent years, the need for sharing data containing user details is becoming a huge necessity. Maintaining those data becomes a complex task. In our project, we use a technique called "**Bit Exchanging Method**" where the data are encrypted so that they can be protected from the adversaries. The updated records needed to be checked often so that they can be used by the encryption techniques. We use a search so called as LBS which a breakthrough concept and technology which offers us an innovative search based on the user current location. They help us to find the user's nearby pizza shop, restaurant, colleges, or any other service stations. Location based service provides the set of service which provides the geographic location of the user. Our project revolves around the HTML5 Geo Location which is an API used to find the location of the user. We utilize k closest neighbor questions where the portable client inquiries the area based specialist organization about surmised k closest purposes of enthusiasm on the premise of his present area. The installing of situating abilities in cell phones encourages the development of area based administrations which is considered as the following "executioner application" in the remote information advertise. Compared with our existing work, our solutions are efficient and provide secured privacy. Examinations have demonstrated that our answer is proper for KNN inquiries.

Keywords: *Bit Exchange; decryption; encryption; Killer application; KNN*

1. Introduction

In recent years the hunger for protection safeguarding information examination and information distributing have gotten colossal consideration as various promising methodologies for sharing information and keeping up singular security have been presented. Consider the Example in versatile correspondence; spatial inquiries represent a genuine danger to client area security on the grounds that the area of a question may uncover touchy data about the portable client. In this work, examine inexact k Nearest Neighbor questions where the portable client inquiries the Location-Based Service supplier about rough k closest Points of Interest on the premise of his present area. Proposed an essential arrangement and a non specific answer for the versatile client to save his area and inquiry protection in estimated KNN inquiries. The implanting of situating abilities in cell phones encourages the rise of Location Based Services which is considered as the following executioner application in the remote information advertises. LBS enable customers to inquiry a specialist co-op in a universal way, with a specific end goal to recover nitty gritty data about purposes of enthusiasm for their region.

The proposed arrangements are fundamentally based on the **Bit Exchanging Method** and can give both area and question protection. To safeguard question security, this fundamental arrangement enables the portable client to recover one kind of POIs, for instance, inexact k closest auto parks, without uncovering to the LBS supplier what sort of focuses is recovered. Proposed bland arrangement can be connected to various discrete sort traits of private area based inquiries. Proposed generic solution can be applied for User Sensitive information. The data's are read in encrypted format using Bit Exchanging Method. This method uses XOR operation to read the queries. A protection saving operation show for the versatile business partnership giving area based administrations is set up. Going for keeping the touchy homogeneity assault, an obscurity display for delicate data is characterized formally. We secure the versatile client's area, identifier and other Sensitive data. At last, the accessibility of the security saving calculation proposed.

2. Objective

The main objective of the project is to ensure the client security information at whatever point the looking questions are prepared with the end goal that information beneficiary including the administrator won't have the capacity to see the protection of the individual records gave by the client.3. SCOPE

The Scope-full areas where this project can be efficiently implemented and that suits well in providing locations based on Point of Interest.

4. Related Works

Haibo Hu at al proposed (2011), Question preparing that jam both the information protection of the proprietor and the inquiry security of the customer is another exploration issue. It demonstrates expanding significance as distributed computing drives more organizations to outsource their information and

questioning administrations. Be that as it may, most existing examinations, including those on information outsourcing, address the information security and question protection independently and can't be connected to this issue. In this paper, they propose an all encompassing and productive arrangement that involves a protected traversal structure and an encryption conspire in light of security homomorphism. The structure is adaptable to extensive datasets by utilizing a file based approach. In light of this system, we devise secure conventions for handling run of the mill questions, for example, k-closest neighbor inquiries (KNN) on R-tree record. Additionally, a few enhancement strategies are displayed to enhance the productivity of the question handling conventions. Our answer is checked by both hypothetical examination and execution consider.

B. Yao, at al (2013) suggested, for as long as decade, inquiry preparing on social information has been considered widely, and numerous hypothetical and viable answers for question handling have been proposed under different situations. With the current fame of distributed computing, clients now have the chance to outsource their information and in addition the information administration undertakings to the cloud. Be that as it may, because of the ascent of different protection issues, touchy information (e.g., therapeutic records) should be encoded before outsourcing to the cloud. Also, inquiry preparing errands ought to be taken care of by the cloud; generally, there would be no good reason for outsource the information at the primary spot. To process inquiries over scrambled information without the cloud regularly unscrambling the information is an exceptionally difficult undertaking. We concentrate on unraveling the k-closest neighbor (KNN) inquiry issue over scrambled database outsourced to a cloud: a client issues an encoded question record to the cloud, and the cloud restores the k nearest records to the client. They initially show a fundamental plan and exhibit that such a guileless arrangement isn't secure. To give better security, we propose a safe KNN convention that ensures the secrecy of the information, client's information inquiry, and information get to designs. Additionally, they exactly break down the productivity of our conventions through different trials. These outcomes demonstrate that our safe convention is exceptionally productive on the client end, and this lightweight plan enables a client to utilize any cell phone to play out the KNN inquiry.

R. Schlegel at al (2015) proposed, Location based service requires user to report their location to untrusted server to obtain services based on the location which affect their privacy. In existing system, the limitation is fully trusted server provides limited guarantee. For the future enhancement we will expand this system by giving location snapshot. In any emergency case, it will provide user module in case user did not register to the system.

X. Yi, R. Paulet , E. Bertino, V. Varadharajan (2015) suggested, the portable client questions the area based administrations about the k closest neighbor on the premise of the present areas. The LBS supplier forms the inquiries of the client in view of the area of the client. The future work is to execute the conventions in the cell phones. Security Analysis demonstrated that we have area protection, client security and information security. Execution demonstrated that convention performs superior to anything PIR based question convention as far as computational and correspondence overhead. The structure of information outsourcing was first presented, in which an information proprietor outsources its information to an outsider specialist co-op who is in charge of noting the information inquiries from either the information proprietor or different clients. When all is said in done, there are two security worries in information outsourcing: information protection and question respectability. Spatial questions represent a genuine risk to client area protection on the grounds that the area of an inquiry may uncover delicate data about the portable client. The current PIR based LBS inquiry conventions as far as both parallel calculation and correspondence overhead. To protect question security, this essential arrangement enables the versatile client to recover one sort of POIs, for instance, inexact k closest auto parks, without uncovering to the LBS supplier what kind of focuses is recovered.

5. System Analysis

Prevention of data is important in the distributed environment. Maintaining privacy and preventing the sensitive information from the attackers is the basic necessity. Whenever the searching queries are processed, the user details are needed to be protected such that the admin will not be able to view the privacy of the individual records provided by theuser.

5.1 Existing System

The embedding of positioning capabilities in mobile devices facilitates the emergence of Location Based Services, which is considered as the next “killer application” in the wireless data market. LBS allow clients to query a service provided in a ubiquitous manner, in order to retrieve detailed information about points of interest in their vicinity. The LBS provider processes spatial queries on the basis of the location of the mobile user. Location information collected from mobile users, knowingly and unknowingly, can reveal far more than just a user’s latitude and longitude.

The main differences between our previous work and our current work are: The previous work fixed the number of nearest neighbors k. The current work allows any number of nearest neighbors k up to K, where K is a constant; the previous work defined location privacy which implied query privacy. The current work defines location and query privacy separately; the current work uses RSA to achieve the data privacy and support sequential queries; the current work adds a generic solution for multiple discrete types attributes of private location-based queries; In addition, we have added some experiments for variable k.

5.1.1. Limitation of Existing System

- ✓ User data is not secure because knowingly or unknowingly the data may be revealed far more than latitude and longitude.
- ✓ The individual LBSPs often have very small data sets comprising POI reviews.

This would largely affect the usefulness and eventually hinder the more prevalent use of spatial top-k query services.

5.2 Proposed System

This project is devoted to tending to this testing issue of confirming moving kNN questions. This work, enhance the best validation strategy and demonstrate that it accomplishes VO-optimality. This optimality idea ensures that the VO contains the base information focuses and tree sections (regarding the given tree). Additionally present new streamlining strategies for decreasing the calculation cost and the communication cost of our authentication method

In our proposed system we are using bit exchanging method is an encryption technique. If the user enters a place or location he requests the query to the service provider. It will provide the service based on the available location. If the location is not available, it updates the new query in its registry. It uses encrypted format to protect the user privacy data. Bit Exchange Method (BEM) uses XOR operation and right shift operation.

5.2.1. Advantages of Proposed System

- ✓ Computation optimization that reduces the server and the client CPU time
- ✓ VO compression that reduces the size of each VO

- ✓ Authentication method achieves low communication cost and CPU overhead.

6. System Architecture

In this system, the user login to search for the places. These queries are stored in an encrypted form in database. Whenever the admin login to insert places, he can view the queries in encrypted format. Bit Exchanging Method is used to decrypt the queries.

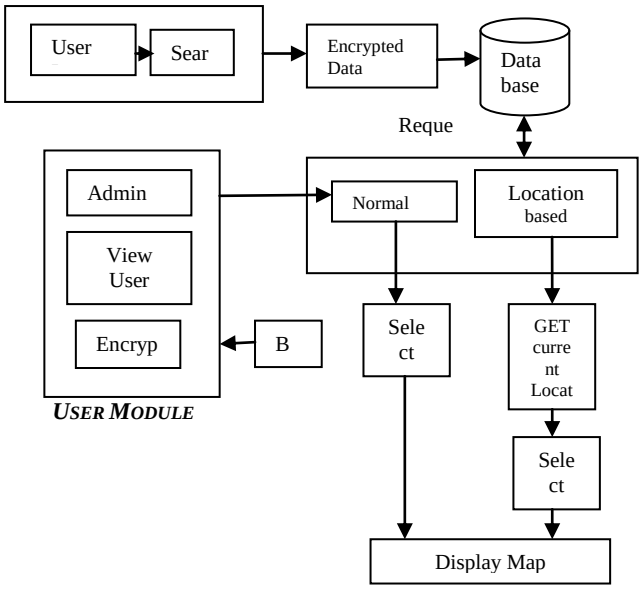

Fig: Architecture of Location and

All users are travel on the underlying network and they also hold privacy policies which specify the privacy requirements of each user. Before accessing or searching for the details, the user should have the account in the applications else they should register first. Once the registration is completed, they can login. User may allow to search, if their login is valid otherwise it shows "invalid details". Once they are valid, they can search for the places based on normal search or through location based search.

6.1 Admin Module

In this module admin needs to insert the places according to the user's requirement. Before inserting the places, they needed to login. Once the login is successful, they can add places and view user queries in an encrypted format. The admin cannot be able to view the user queries as they are in encrypted. This is a major advantage in our work. We use BEM to decrypt the queries so that the user queries are updated. Hence the third party can't access the user's privacy details.

6.2. Normal Search Module

In this module user can search the location. The admin must login to insert the locations for user search. These locations are stored in the database. Once they are stored, the user must login and search for the needed places. These searching queries are in the encrypted format so that they must be decrypted by the admin to view the user queries. The user can get the locations with the desired map displayed.

6.3 Location Based Service

Location-based service providers play the role of spatial data maintainers and spatial query processors in our system. The same procedure is followed as the normal search. The admin must be loginned to insert places previously and whenever the user wants to search for the places, they must do LBS Search. The Latitude and Longitude are displayed based on our current locations. With the help of these latitude and longitude, user can find the nearest places with respect to their locations and the desired map is displayed

Bit Exchanging Method

Encryption gone up against the mystery message records utilizing straightforward piece moving and XOR operation. The bit trade technique is presented for encoding any record. The accompanying advances are engaged with Bit Exchange Method: A Bit Exchange strategy works on at least one piece examples or double numerals at the level of their individual bits. It is a quick, basic activity straightforwardly bolstered by the processor, and is utilized to control esteems for correlations and estimations. Encryption gone up against the mystery message records utilizing straightforward piece moving and XOR operation. The bit trade strategy is presented for scrambling any record. Here the information's are perused one by one and changed over to 8 bits. These 8 bits are partitioning into 4 bits and performed XOR operations. These means are rehashed until the point that the questions are encoded. Coherent movements can be valuable as proficient approaches to perform duplication or division of unsigned whole numbers by forces of two. Moving ideal by n bits on unsigned parallel number has the impact of isolating it by 2n Rounding towards 0.

6.4 Coding

Once the outline parts of the framework are settled the framework goes into the coding and testing stage. The coding stage brings the real framework vigorously by changing over the outline of the framework into code in a given programming dialect. Along these lines, a great coding style must be taken at whatever point changes are required it can be effectively screwed into the framework.

6.5 Coding Standards

Coding measures are rules to programming that spotlights on the physical structure and appearance of the program. They make the code less demanding to peruse, comprehend and keep up.
This period of the framework really actualizes the outline created amid the plan stage. The coding determination ought to be such that any software engineer must have the capacity to comprehend the code and can achieve changes, at whatever point felt vital.
A portion of the standard expected to accomplish the previously mentioned goals are as per the following:

- ✓ Program ought to be straightforward, clear and straightforward.
- ✓ Naming Conventions.
- ✓ Value Conventions.
- ✓ Script and remark techniques.
- ✓ Message box arrange.

7. Conclusion and Future Enhancement

In this project, a new type of technique has been considered called as "Bit Exchanging Method" for the protection of user information. Establishing efficient privacy techniques is enough to prevent the privacy disclosures by any adversaries. The algorithm is introduced with adaptive privacy checking so called as Encryption technique. The performance achieves greater heights than the existing PIR Search. Our Encryption achieves better efficiency and security than the existing privacy techniques.
There are many outstanding examination inquiries on characterizing protection for various imperatives. It additionally

remains an inquiry to address and model the information learning when information are utilized as a part of a scrambled procedure. Our future work is to actualize our convention on cell phones.

References

[1] R. Schlegel, C. Chow, Q. Huang, D. Wong. User-defined privacy grid system for continuous location-based Services. IEEE Transactions on Mobile Computing, (Jan. 2015).

[2] X. Yi, R. Paulet , E. Bertino, V. Varadharajan. Practical k nearest neighbor queries with location privacy. In Proc. ICDE (2015).

[3] G. Ghinita, R. Rughinis. An efficient privacy-reserving system for monitoring mobile users: making searchable encryption practical. in Proc. ACM CODASPY (2014).

[4] Y. Elmehdwi, B. K. Samanthula, W. Jiang. Secure k-nearest neighbor query over encrypted data in outsourced environments. In Proc. ICDE (2014).

[5] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. Privacy preserving and content-protecting location based queries(2013).

[6] B. Yao, F. Li, and X. Xiao. Secure nearest neighbor revisited. In Proc. ICDE (2013).

[7] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino. Privacy preserving and content-protecting location based queries. In Proc.ICDE (2012).

[8] B. Palanisamy and L. Liu. Mobimix: Protecting location privacy with mix-zones over road networks. In Proc. ICDE (2011).

[9] Haibo Hu, Jianliang Xu, Chushi Ren, and Byron Choi, Processing Private Queries over Untrusted Data Cloud through Privacy Homomorphism, In Proc. ICDE (2011).

[10] S. Papadopoulos, S. Bakiras, D. Papadias. Nearest neighbor search with strong location privacy. In Proc. VLDB (2010).

[11] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino. Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection. GeoInformatica 15(14): 699-726, (2010).

[12] B. Bamba, L. Liu, P. Pesti, and T. Wang. Supporting anonymous location queries in mobile environments with PrivacyGrid. In Proc. WWW (2008).

[13] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan. Private queries in location-based services: Anonymizers are not necessary. In Proc. ACM SIGMOD (2008).

[14] A. Khoshgozaran and C. Shahabi. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In Proc. SSTD (2007).

[15] R. Ostrovsky and W. Skeith. A survey of single-database private information retrieval: techniques and applications. In Proc. PKC (2007).