International Journal of Engineering Research And Management (IJERM)
ISSN: 2349- 2058, Volume-04, Issue-05, May 2017

Efficiency and Privacy-Preserving In Spatial Range Query over Encrypted Data

Prof. Shweta Sidnal, Prof. Kavita D Hanabaratti

Abstract— **The aim of safe location based application to outsource the location based service (LBS) data from the LBS provider to the cloud and from the cloud to the LBS user which protects the privacy related issues of the LBS data. Initially LBS user query for a place to the LBS provider, LBS provider in turn upload the details to the cloud but in the form of encrypted text to prevent the cloud from stealing the data. LBS users in turn decrypt the details by the personal password send by the LBS provider to the LBS user. When the query of the LBS user matches the details in the cloud the LBS user will retrieve the details and make use of it. With the pervasiveness of smart phones, location based services have received considerable attention and become more popular and vital recently. However, the use of LBS also has a potential threat to user's location privacy. Aiming at spatial range query, popular LBS providing information About Points of Interest, an effective and privacy-preserving LBS solution, called EPSQ is developed. To reduce query latency, further a privacy-preserving tree index structure called SS tree is used in EPSQ. Detailed security analysis confirms the security properties of EPSQ.**

INTRODUCTION

A few years ago, location-based services (LBS) were used in military only. Today, thanks to advances in information and communication technologies, more kinds of LBS have appeared, and they are very useful for not only organizations but also individuals. Let us take the spatial range query, one kind of LBS that will be focused in the proposed system, as an example. Spatial range query is a widely used LBS, which allows a user to find points of interest (POIs) within a given distance to his/her location, i.e., the query point. As illustrated in Fig. 1, with this kind of LBS, a user could obtain the records of all restaurants within walking distance (say 500 m). Then, the user can go through these records to find a desirable restaurant considering price and reviews. While LBS are popular and vital, most of these services today including spatial range query require users to submit their locations, which raises serious concerns about the leaking and misusing of user location data. For example, criminals may utilize the data to track potential victims and predict their locations. For another example, some sensitive location data of organization users may involve trade secret or national security. Protecting the privacy of user location in LBS has attracted considerable interest. However, significant challenges still remain in the design of privacy-preserving LBS, and new challenges arise particularly due to data outsourcing. In recent years, there is a growing trend of outsourcing data including LBS data because of its financial and operational benefits.

With overall view, the Location Based Service applications can be categorized as:

Navigation applications such as Route description, Turn-by-turn navigation.

- Safety and emergency applications like nearest medic center, Emergency calls, Warning about unsafe areas.
- Tracking applications such as Find a friend, Asset tracking etc.
- Information service applications like Traffic information, City Guide, Parking, Maps etc.
- Operator & Tariff applications like Traffic measurements, Network planning.

EXISTING SYSTEM

- There are already some solutions for privacy preserving spatial range query.
- Protecting the privacy of user location in LBS has attracted considerable interest. However, significant challenges still remain in the design of privacy-preserving LBS, and new challenges arise particularly due to data outsourcing. In recent years, there is a growing trend of outsourcing data including LBS data because of its financial and operational benefits.
- Lying at the intersection of mobile computing and cloud computing, designing privacy- preserving outsourced spatial range query faces the challenges.

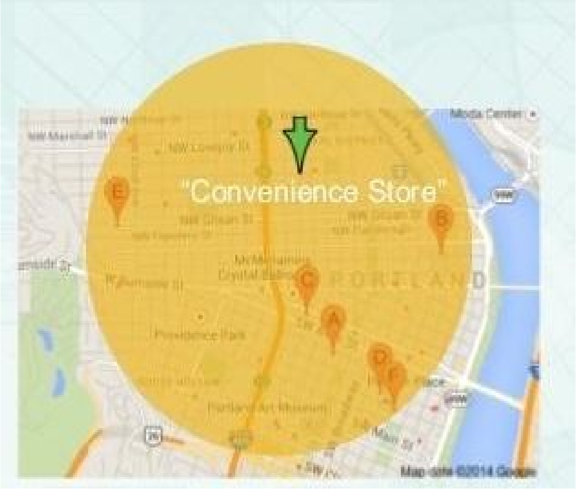

Fig1.Example of Spatial range query

Manuscript received May 17, 2017

Prof.Shweta Sidnal, Dept. of MCA, KLE RL Science Institute , Belagavi
Prof. Kavita D Hanabaratti, Dept. of Computer science and engineering Gogte Institute of technologe , Belagavi

There are four kinds of privacy-preserving queries over Points of Interests which are as follows

- Spatial range query: which allows a user to find points of interest (POIs) within a given distance to user location?
- Nearest neighbour (NN) query: which allows a user to find the nearest point of interest to user location?
- K nearest neighbours (KNN) query: which allows a user to find the K nearest point of interests to user location
- Multidimensional range query: This allows a user to find the POIs in a rectangular area instead of a circular area.

Existing Solutions for Outsourced LBS

1. **Privacy-Preserving Spatial Range Query Based on Coordinate Transformation:**

In the solution based on coordinate transformation, the coordinates of queries and POIs in the original coordinate system are transformed to new coordinates in a new coordinate system. After the transformation, the distance information of any two points is still preserved. Coordinate transformation is very efficient, and the return results are accurate. However, solutions designed based on coordinate transformation would be vulnerable to known-sample attacks.

Disadvantages:

- It is difficult, expensive and time-consuming for service providers to circumvent the protection mechanisms on a large scale in order to obtain reliable location information of all users.
- It adds complexity to the processing of location information and generating overhead with respect to bandwidth, storage capacity and processing time.
- Development of strategies for client applications to keep track of the different coordinate systems is very difficult.

2. **Privacy-Preserving POI Query Based on PIR:**

PIR-based solutions can protect the privacy in both public LBS and outsourced LBS. Private information retrieval (PIR) is privacy primitive hiding the retrieved data item's ID from the database servers. Because the data items being retrieved are hidden from the database servers, whether two queries' results are the same or not are undetectable. Therefore, PIR-based solutions are resilient to access-pattern attacks. PIR can be used to realize all the four kinds of POI queries. However, PIR is very communicative and computationally costly.

Disadvantages:

- PIR requires linearly scanning all POI records including their location data (coordinates and radii) and non location data.
- LBS user must additionally access the LBS database's index data in a privacy preserving manner.
- PIR can retrieve records if given their IDs. To support spatial range query, an LBS user should obtain nearby POIs record IDs from index data in a privacy-preserving manner.

PROBLEM DEFINITION

There is necessity to protect the privacy of user location in LBS. The –***Efficiency and Privacy Preserving in Spatial Range Query Over Encrypted Data***‖ is a technique which protects the user location information and efficiently search for Point of Interest in the given area. Designing Privacy Preserving Outsourced Spatial range query faces the Challenges:

1. Querying encrypted LBS data
2. The resource consumption in mobile devices
3. The efficiency of POI searching
4. Security

PROPOSED SYSTEM

- This is an efficient solution for privacy-preserving spatial range query named EPSQ, which allows queries over encrypted LBS data without disclosing user locations to the cloud or LBS provider.
- To protect the privacy of user location in EPSQ, design a novel predicate-only encryption scheme for inner product range (IPRE scheme for short), is the first predicate/predicate-only scheme of this kind. To improve the performance, a privacy preserving index structure named ˆ ss-tree is also designed.
- The IPRE, which allows testing whether the inner product of two vectors is within a given range without disclosing the vectors. In predicate encryption, the key corresponding to a predicate f can decrypt a ciphertext if and only if the attribute of the ciphertext x satisfies the predicate, i.e., f(x) = 1. Predicate-only encryption is a special type of predicate encryption not designed for encrypting/decrypting messages. Instead, it reveals that whether f(x) = 1 or not. Predicate-only encryption schemes supporting different types of predicates have been proposed for privacy-preserving query on outsourced data.
- The EPSQ, an efficient solution for privacy preserving spatial range query. In particular, this shows that whether a POI matches a spatial range query or not can be tested by examining whether the inner product of two vectors is in a given range. The two vectors contain the location information of the POI and the query, respectively. Based on this discovery and IPRE scheme, spatial range query without leaking location information can be achieved. To avoid scanning all POIs to find matched POIs a novel index structure named ˆ ss-tree is used, which conceals sensitive location information with our IPRE scheme.
- This technique can be used for more kinds of privacy preserving queries over outsourced data. In the spatial range query discussed in this work, Euclidean distance is considered, which is widely used in spatial databases. IPRE scheme and ˆ ss-tree may be used for searching records within a given weighted Euclidean distance or great-circle distance as well. Weighted Euclidean distance is used to measure the dissimilarity in many kinds of data, while great-circle distance is the distance of two points on the surface of a sphere.

DIFFERENT INDEX STRUCTURES

- **SStree (similarity search tree) -** Every disk node in the structure consists simply of an array of the SSElem. both internal nodes and leaf nodes use the above structure. If the SSElem is a leaf element, data holds the data for that leaf, and centroid holds the object's feature vectors, and radius bounds the object's extent in feature space (this was zero in our tests on point data). If SSElem is an internal node, then its information is defined by its children.
- **SR-tree (Spherel Rectangle-tree)** – **A** region of the SR-tree is specified by the intersection of a bounding sphere and bounding rectangle. Incorporating bounding rectangles permits neighbourhoods to be partitioned into smaller regions than the SS-tree and improves the disjointness among regions. This enhances the performance on nearest neighbour queries especially for high dimensional and non-uniform data. distinctive feature of the SR-tree is that it specifies a region by the intersection of the bounding sphere and the bounding rectangle of underlying points.
- **SH-tree (Super Hybrid tree)** - Because the SH-tree is planned to apply not only for point data objects, but also for extended data object choose no overlap-free space partitioning. This approach easily control objects that cross a selected split position and solve the storage utilization problem. There are three node kinds in the SH-tree: Internal, balanced and leaf nodes.
- **X-tree (extended node tree)** - The X-tree (extended node tree) is a new index structure supporting efficient query processing of high-dimensional data. The goal is to support not only point data but also extended spatial data and therefore, the X-tree uses the concept of overlapping regions. The X-tree therefore avoids overlap whenever it is possible without allowing the tree to degenerate; otherwise, the X-tree uses extended variable size directory nodes, so-called supernodes. In addition to providing a directory organization which is suitable for high-dimensional data, the X-tree uses the available main memory more efficiently.
- **A-tree (Approximation tree)** - A-tree is the introduction of Virtual Bounding Rectangles (VBRs), which contain and approximate MBRs and data objects, respectively. VBRs can be represented rather compactly, and thus affect the tree configuration both quantitatively and qualitatively. Firstly, since tree nodes can install large number of entries of VBRs, fanout of nodes becomes large, thus leads to fast search. More importantly, this has a free hand in arranging MBRs and VBRs in tree nodes. In the A trees, nodes contain entries of an MBR and its children VBRs. Therefore, by fetching a node of an A-tree, the information of exact position of a parent MBR and approximate position of its children can be obtained.

CHALLENGES OF THE PROPOSED SYSTEM

1. **Efficiency:** Spatial range query has stringent performance requirements. A good solution should not consume many resources of mobile LBS users, and the POI search latency should be acceptable for online query.
2. **Accuracy:** It is desirable that a query result contains the exact records matching the query. False negatives would hurt user experience, while false positives would increase communication cost. Additional computational cost is also required at the user side to filter out false positives.
3. **Security:** The proposed solution should be resilient to ciphertext-only attacks and known sample attacks. An accurate and efficient solution for spatial range query already exists, which is resilient to ciphertext-only attacks but not to known-sample attacks and more powerful attacks. The proposed solution should be more secure than the solution in.

RELATED WORK

1. EPLQ an efficient and privacy-preserving location-based query solution[1] which depends on predicate-only encryption scheme for inner product range (IPRE), which can be used to detect whether a position is within a given circular area in a privacy-preserving way and it allows to test whether inner product of two vectors is within given range or not without disclosing the vectors. EPLQ allows queries over encrypted LBS data without disclosing user locations to the cloud or LBS provider. It uses a index data structure to store and access the data efficiently.
2. Anonymity can provide a high degree of privacy, save service users from dealing with service providers privacy policies, and reduce the service provider's requirements for safe guarding private information. This is a public-key systems that support comparison of queries. On encrypted data as well as more general queries such as subset queries. These systems support arbitrary conjunctive queries without leaking information on individual conjuncts. In addition, a general framework was introduced for constructing and analyzing public-key systems supporting queries on encrypted data[2].
3. In Secure KNN computation on encrypted database[3] , service providers like Google and Amazon are moving into the Software as a Service business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruited businesses to run applications on their respective platforms. To enforce security and privacy on such service model, there is need to provide protection to the data running on the platforms. Traditional encryption methods that aim at providing unbreakable protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. In Secure KNN computation on encrypted database the general problem of secure computation on an encrypted database and propose a SCONEDB (Secure Computation ON an Encrypted DataBase) model, which captures the execution and security requirements. The focus was on the problem of k-nearest neighbor (KNN) computation on an encrypted database. A new asymmetric

scalar-product- preserving encryption (ASPE) that preserves a special type of scalar product was developed. APSE is used to construct two secure schemes that support KNN computation on encrypted data; each of the schemes shows resistance of practical attacks of a different background knowledge level, at a different overhead cost.

4. Coordination transformation is a Private [4], a distributed architecture for anonymous location-based queries, which addresses the problems of existing systems. (i) Develop a superior K-ASR construction mechanism that guarantees query anonymity even if the attacker knows the location of all user. (ii) Introduce a distributed protocol used by mobile entity to self-organize into a fault-tolerant overlay network. In Private, K-ASRs are built in a decentralized fashion, therefore the bottleneck of the centralized server is avoided. Since the state of the system is distributed, Private is resilient to attacks. This approach hurts the accuracy and timeliness of the responses from the Server. But the challenge of providing strong privacy guarantees while maintaining high data accuracy of time-series location data. The key features of this are: 1. a novel time-to-confusion metric to evaluate privacy in a set of location traces. 2. an uncertainty-aware privacy algorithm that can guarantee a specified maximum time-to-confusion.
5. Encryption is a well established technology for protecting sensitive data. However, once encrypted, data can no longer be easily queried aside from exact matches. Order- preserving encryption scheme for numeric data allows any comparison operation to be directly applied on encrypted data. Query results produced are sound and complete. The scheme handles updates gracefully and new values can be added without requiring changes in the encryption of other values. It allows standard database indexes to be built over encrypted tables and can easily be integrated with existing database systems. The scheme has been designed to be deployed in application environments in which the intruder can get access to the encrypted database, but does not have prior domain information such as the distribution of values and cannot encrypt or decrypt arbitrary values of his choice. The encryption is robust against estimation of the true value in such environments[5].
6. FINE framework is based on the CP-ABE scheme. In this framework, LBS data are outsourced to a cloud server after encryption. Although the framework can ensure the confidentiality of LBS data, the search patterns will lead to the leakage of user location privacy, because the trapdoors generated from the locations are steady, which means trapdoors are always the same for the same location. It is easy for an attacker to count the frequency of a specific trapdoor and identify the known locations. In addition, this method is not efficient due to the low efficiency of the public encryption [6].
7. Find me if you can is a suite of fine-grained privacy-preserving location query protocols (PLQP) by applying Paillier's cryptosystem. It can solve the privacy issues in existing LBS applications. However, once there is an LBS request, the PLQP needs very frequent interaction between the publisher and the querier and much computation cost. In mobile sensing service systems, most queriers access the social networks via smart phones. The smart phones have weak power. Hence, it is unacceptable for the publishers to stay online always [7].
8. Homomorphic encryption schemes make it possible to perform arithmetic operations, like additions and multiplications, over encrypted values. This capability provides enhanced protection for data and offers new research directions, including blind data processing. Using homomorphic encryption schemes, a Location-Based Service (LBS) can process encrypted inputs to retrieve encrypted location-related information. The retrieved encrypted data can only be decrypted by the user who requested the data. The technology still faces two main challenges: the encountered processing time and the upper limit imposed on the allowed number of operations. However, the protection of users' privacy achieved through this technology makes it attractive for more research and enhancing. In this paper we use homomorphic encryption schemes to build a fully secure system that allows users to benefit from location-based services while preserving the confidentiality and integrity of their data. Our novel system consists of search circuits that allow an executor (i.e. LBS server) to receive encrypted inputs/requests and then perform a blind search to retrieve encrypted records that match the selection criterion. A querier can send the user's position and the service type he/she is looking for, in en-crypted form, to a server and then the server would respond to the request without any knowledge of the contents of the request and the retrieved records. We further propose a prototype that improves the practicality of our system [8].
9. For indexing spatial data, there actually exist quite a few data structures such as r-tree and ss-tree, and some of them can be used for spatial range query. When such kind of data structures are used for privacy preserving query, location data, e.g., the location data of points, circular areas, rectangular areas, and single-dimension ranges, must be concealed. Since the proposed scheme can conceal location data of points and circular areas, and at the same time ss-tree and some of its variants only need these location data. As SS tree is going to store radius at each node it is very efficient to search point of interest in spatial range queries in location based services. All descendant nodes of a non-leaf node are in the non-leaf node's associated circular area. Searching POI records can be done by scanning the ss-tree from root to leaves [9].

10. PIR framework supports private location-dependent queries, which is based on the theoretical work on Private Information Retrieval (PIR). This framework does not require a trusted third party, since privacy is achieved via cryptographic techniques. This approach achieves stronger privacy for snapshots of user locations; moreover, it is the first to provide provable privacy guarantees against correlation attacks. The framework is used to implement approximate and exact algorithms for nearest-neighbor search. Query execution is optimized by employing data mining techniques, which identify redundant computations. PIR approach suffers reasonable overhead and is applicable in practice [10].

SYATEM DESIGN

SYSTEM ARCHITECTURE

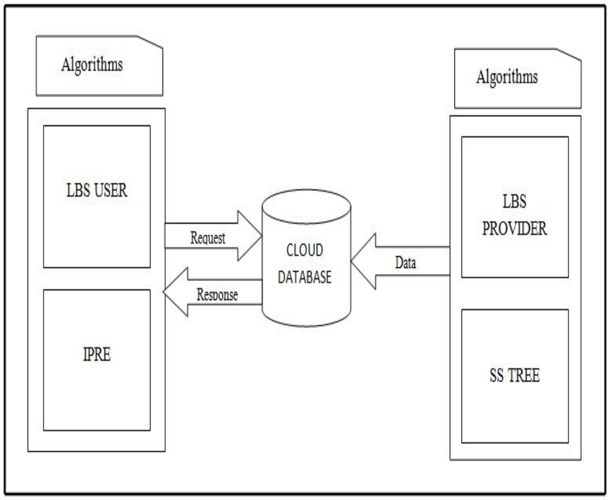

Fig.1 System Architecture

The above diagram specifies architecture of the system which is divided into two blocks. The first block LBS USER is a client which uses IPRE scheme to produce two key vectors for the query over location based service and is sent to the cloud. The second block is the LBS PROVIDER which builds the SS TREE to store the data of the different point of interest and later it sends the data and SS TREE to the cloud to store and execute location based queries from the user. Different algorithms are used to encrypt and decrypt the data.

ALGORITHMS

Encryption Algorithm:

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message. One of the most widely used and efficient encryption algorithm is Advanced Encryption Standard(AES).

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256- bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

Decryption Algorithm:

The AES decryption basically traverses the encryption algorithm in the opposite direction. AES decryption algorithm initially performs key-expansion on the 128-bit key block that creates all intermediate keys which are generated from the original key during encryption for every round.

IMPLIMENTATION

MODULES:

- System Construction Module
- LBS User
- LBS Provider
- Privacy-Preserving Spatial Range Query

MODULES DESCSRIPTION:

System Construction Module

- ❖ The LBS provider has abundant of LBS data, which are POI records. The LBS provider allows authorized users (i.e., LBS users) to utilize its data through location-based queries. Because of the financial and operational benefits of data outsourcing, the LBS provider offers the query services via the cloud. However, the LBS provider is not willing to disclose the valuable LBS data to the cloud. Therefore, the LBS provider encrypts the LBS data, and outsources the encrypted data to the cloud.
- ❖ The cloud has rich storage and computing resources. It stores the encrypted LBS data from the LBS provider, and provides query services for LBS users. So, the cloud has to search the encrypted POI records in local storage to find the ones matching the queries from LBS users.
- ❖ LBS users have the information of their own locations, and query the encrypted records of nearby POIs in the cloud. Cryptographic or privacy-enhancing techniques are usually utilized to hide the location information in the queries sent to the cloud. To decrypt the encrypted records received from the cloud, LBS users need to obtain the decryption key from the LBS provider in advance.

LBS User

- ❖ In this Module, the mobile user sends location-based queries to the LBS provider (or called the LBS server) and receives location-based service from the provider. The mobile user queries the location based service provider about approximate k nearest points of interest on the basis of his current location. In general, the mobile user needs to submit his location to the LBS provider which then finds out and returns to the user the k nearest POIs by comparing the distances between the mobile user's location and POIs nearby. This reveals the mobile user's location to the LBS provider.

LBS Provider

- ❖ In this Module, the LBS provider provides location-based services to the mobile user. LBS allow clients to query a service provider in a ubiquitous manner, in order to retrieve detailed information about points of interest (POIs) in their vicinity (e.g., restaurants, hospitals, etc.). 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.

Privacy-Preserving Spatial Range Query

- ❖ In EPSQ, user queries and the sensitive location information are encrypted with IPRE scheme. A query consists of two tokens associated with two predicate vectors, which contains the LBS user's location information. The LBS user generates two tokens for searching
- ❖ POI records with the proposed IPRE scheme. The two tokens associated with the query area should be generated. Let Ks[0] and Ks[1] be the generated two tokens.
- ❖ The user sends a query to the LBS Service Provider. The LBS Service Provider searches to find all leaf nodes matching the query from the user. The LBS Service Provider returns the corresponding POI records of matched leaf nodes to the user. The LBS user decrypts received POI records with the shared key of the standard encryption scheme.

FUTURE WORK

The efficiency of search can be increased by using the more appropriate index data structures to store and access the data. Complex and more efficient algorithms for encrypting the data should be implemented because cloud computing is growing faster and faster day by day and the computational power of cloud storage is becoming powerful enough to decode the data sent by the service provider.

CONCLUSION

The proposed system EPSQ , an efficient privacy preserving spatial range query solution for smart phones, which preserves the privacy of user location, and achieves confidentiality of LBS data. To realize EPSQ, we have designed an IPRE and a novel privacy-preserving index tree named ss-tree. EPSQ's efficacy has been evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and ciphertext-only attacks. This technique has potential usages in other kinds of privacy preserving queries. If the query can be performed through comparing inner products to a given range, the proposed IPRE and ss-tree may be applied to realize privacy-preserving query. Two potential usages are privacy-preserving similarity query and long spatial range query. In the future, design solutions for these scenarios will be developed and identify more usages.

REFERENCES

[1] Lichun Li, Rongxing Lu and Cheng Huang, –EPLQ: Efficient Privacy-Preserving Location- Based Query Over Outsourced Encrypted Data‖ in IEEE internet of things journal, vol. 3, no. 2, april 2016.

[2] D. Boneh and B. Waters –Conjunctive, subset, and range queries on encrypted data‖ in 4th Theory of Cryptography Conference, TCC 2007,Amsterdam,The Netherlands, 2007

[3] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, –Secure kNN computation on encrypted databases,‖ in Proc. SIGMOD, 2009.

[4] A. Gutscher, –Coordinate transformation—A solution for the privacy problem of location based services?‖ in Proc. 20th Int. Parallel Distrib. Process. Symp. (IPDPS'06), Rhodes Island, Greece, Apr. 25–29, 2006.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu –Order preserving encryption for numeric data‖, in SIGMOD. ACM, 2004.

[6] Shao J., Lu R., Lin X, –FINE: A fine-grained privacy-preserving location-based service framework for mobile devices‖, Proceedings of the IEEE INFOCOM, Toronto, Canada.2014.

[7] Li X.Y., Jung T –Search me if you can: Privacy-preserving location query service‖, Proceedings of the IEEE INFOCOM, Turin, Italy,2013.

[8] Youssef Gahi1, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib –Privacy Preserving Scheme for Location-Based Services‖, Journal of Information Security, 2012.

[9] D. A. White and R. Jain, –Similarity indexing with the ss-tree,‖ in Proc. 12th International.Conference (ICDE), 1996.

[10] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, –Private queries in location based services: Anonymizers are not neces-sary,‖ in Proc. SIGMOD, 2008.

[11] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, –Private informa-tion retrieval,‖ J. ACM, 1998.

[12] F. Olumofin and I. Goldberg, –Revisiting the computational practicality of private information retrieval,‖ in Financial Cryptography and Data Security. New York, NY: Springer, 2012.

[13] Norio Katayama and Shin'ichi Satoh, "The SR-tree: An Index Structure for High- Dimensional Nearest Neighbor Queries‖, in 'Proceedings of tlie 1997 ACM SIGMOD International Conference on Management of Data, 1997.

[14] Dang Tran KHANH, Josef KÜNG, Roland WAGNER, ―The SH-tree: A Super Hybrid Index Structure for Multidimensional Data‖.

[15] Stefan Berchtold, Daniel A. Keim and Hans-Peter Kriegel, –The X-tree: An Index Structure for High-Dimensional Data‖, in Proceedings of the 22nd VLDB Conference Mumbai (Bombay), India, 1996.