International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 9 – DECEMBER 2016.

E2SQ-LBS: EXPLORING AND SECURING THE SPATIAL QUERIES OF LOCATION BASED SERVICES OVER PUBLIC CHANNEL

PITHANI SATYA SAMEERA[#1] and NALLI SUJATHA KUMARI[*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science , JNTUK,A.P, India.*

[*] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— A novel distributed framework for cooperative location-based data information and sharing has been widely studied in the location based services. In this paper, we propose an enhanced E2SQ-LBS scheme, which securely searches the data by the assistance of Google Map. Based on the Point of Interest (POI), the frequently searched data will be analyzed and ranked. The top k queries are frequently updated in order to satisfy the user's requirements. This paper presents three novel plans for clients to recognize fake spatial depiction and moving top-k question results as a push to cultivate the useful arrangement and utilization of the proposed framework. An experimental design and analysis shows the effectiveness of the systems.**

***Index Terms*— Spatial top-k query, location-based service, security, POI**

I. INTRODUCTION

With an explosive growth in internet, Location monitoring becomes an important part in organization. In the world of smartphones, the Location based Services (LBS) plays a vital role in the mobile devices [1]. The security over the outsourced data in the cloud remains as a big concern. The spatial queries act as the basic building block between the query processing and relational database management system. Data confidentiality [2] is the most important security concerns.

In modern society all smart phones have internet access there by acquiring exact location with help of positioning software [3]. For users who are new to a region it is convenient to access and share information regarding POI's [4] like restaurants, hotels, grocery stores, coffee shops. Most of the LBSP's provide a location based query processing which have a drawbacks like limited datasets, POI reviews and multiple ratings for single POI by different LBSP's .sometimes even if the LBSP's are not malicious they may return query results under the effect of various type of attacks like submission of fake reviews for the same POI by the same attacker [5]. This leads to unwise decisions made from the query results.

In this paper, we propose exploring and securing the spatial queries of Location Based Services (E2SQ- LBS) via public channel. Firstly, the data is collected from the registered users. Depends on the rating information, the topmost searched queries are sorted out. It mingles with the Google Map to acquire the location information. The rest of the paper is organized into four sections. Section II describes about the related work done by other researchers. Section III describes about the proposed design of the E2SQ-LBS. Section IV describes the experimental analysis of the E2SQ-LBS. Atlast, concluded in Section V.

II. RELATED WORK

The state of the art in Location Based Services (LBS) includes data owners, data clients and the service providers. Most of the work concerned about the data outsourcing with limited study. The architecture of the data outsourcing is discussed in [4]. Here the data owner outsources their data to the third party auditor, who is responsible to provide the solution for the entered queries. When the data is being outsourced, there rise two security issues like data privacy and query integrity. In order to maintain the privacy of the data, the outsourced data should be encrypted by efficient techniques. Then the study was further extended to the range queries over encrypted data using bucketization approach [6] [7] and which is further extended in [8]. A multidimensional arrangement of range queries for the encoded data was studied by shi et al [9].

Presently, the advent of fine-grained structure was used for examining the encrypted data [10-12]. As this study is focused on the outsourced data, the publicly accessible location based data is required for privacy protection. Here the data schemes ensure the integrity of the query. While outsourcing the data, the owner sends both the data as well as its signature to the service provider. Several techniques were proposed for the signature verification [13-15]. The signature scheme is further enhanced to the chaining system of data in [5] 16] [17] [18]. The above discussed study doesn't discuss about the spatial top k queries. It is studied with the POI in the query region.

Secure remote query processing in the wireless sensor networks [20], [21], [22], [23], [24] is also loosely related to our work here. These schemes assume that some master nodes are in charge of storing data from regular sensor nodes and answering the queries from the remote network owner. Various techniques were proposed in [20], [21], [22], [23] to ensure data privacy against master nodes and also enable the network owner to verify range-query integrity. Moreover, Zhang et al. [24] proposed efficient techniques for the network owner to validate the integrity of top-k queries.

III. PROPOSED WORK

In this section, we explain about the enhanced model to secure the spatial queries transformed via public channel. The system is executed in four phases:

a) System Model
b) Location based service provider
c) Query processing
d) Query result verification

A. *System Model:*

This model contain data collector module. The task of this module is to acquire the rating information posted by the uses. It operates based on the location of the users. The information is collected from the registered users. Next is the user module. In this step, the user registers with the service system and details like login credentials etc. The registered user integrates with the Google Map and the landmark associated keyword.

B. *Location Service Provider:*

This module contains program-level services that contain location control features. Based on the geographic position of the mobile devices, the credentials about the user are collected. This service can also apply to the context like health, work, personal life etc. The location information like longitude and latitude of the exact location is provided.

C. *Query Processing:*

Using the data from the LBSP module, POIs are used for query processing. The Merkle Hash Tree (MHT) contains the Merkle Hash function and constructs the signature based hash tree.

D. *Query result verification:*

A small plug-ins is developed by the data collector and installed on the web browser. It points to the work by embedding or combining some information among nearby zones to reduce the amount of information return to the user. This query is to return the k highest ranked answer or data sets quickly and efficiently.

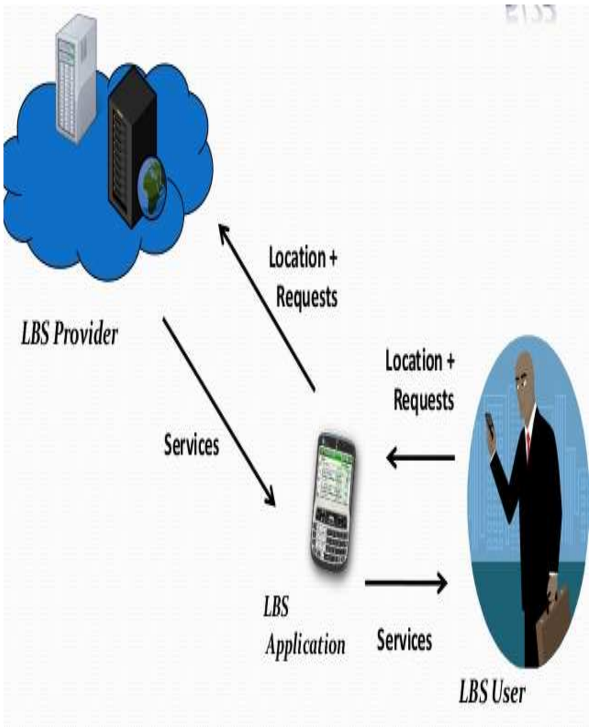

Fig.1. System Architecture

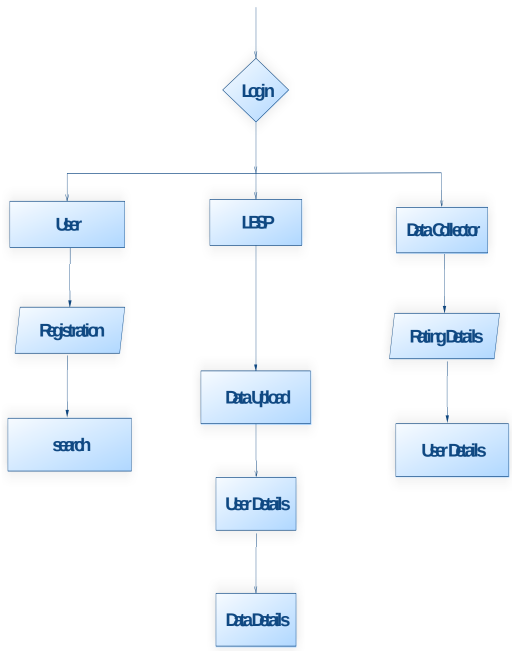

Fig.2. Working flow of each process.

IV. EXPERIMENTAL RESULTS

In this section, we explain about the experimental analysis of the study. This approach intends to provide a signature authentication that ensures data integrity and authentication for the outsourced data. It can't assure the completeness of the result sets. Their mechanism helps users verify that query results are both complete and authentic. In addition, the challenge token scheme is for a server running outsourced databases to provide a proof of the actual query execution, which is then checked at the client side for integrity verification. Compared to, the scheme also supports more query types without assuming that all the records are sorted. Nonetheless, none of the techniques are specifically designed for spatial databases.

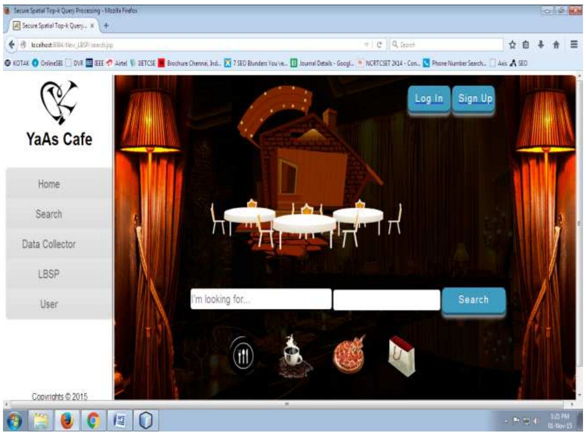

Fig.3. Data collection of the spatial databases

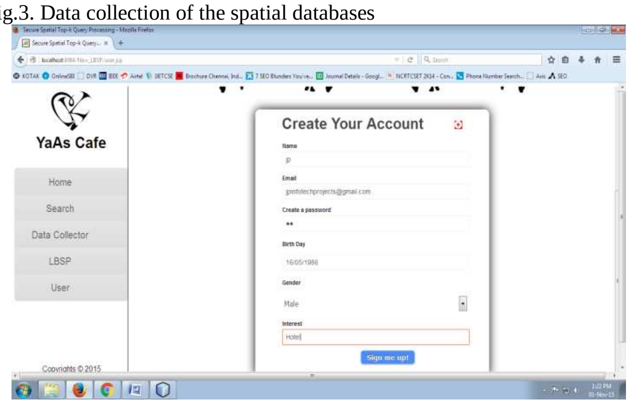

Fig. 4. User specifying the queries

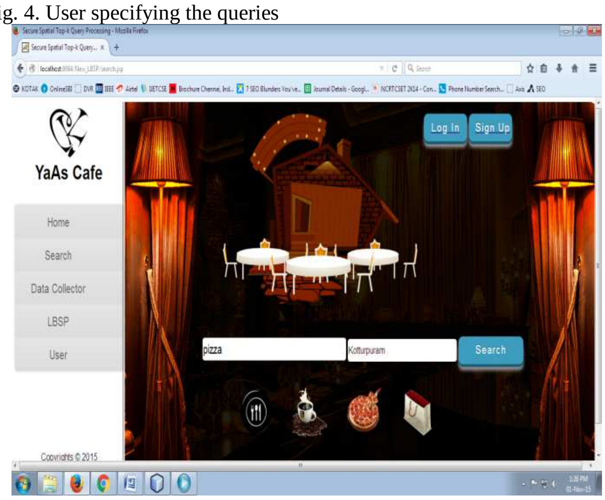

Fig.5. Searching for the data

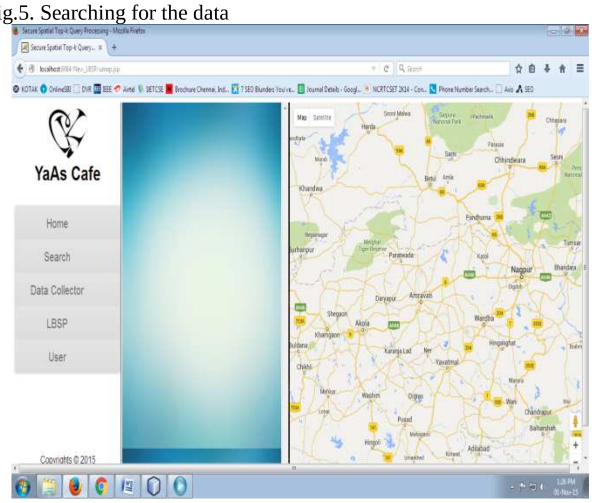

Fig.6. With the use of Google Map, the user specified query is found out.

V. CONCLUSION

In this paper, we have studied the problem of authenticating E2SQ-LBS. A novel distributed system for cooperative location-based information generation and sharing. It projected three novel schemes to modify secure top-k question process via un-trusted LBSP. With the use of Google Map, the user specified query is searched and retrieved. The top k queries are analyzed and ranked behind the relational database systems. The projected platform itself wherever push and pull LBS services are often integrated on a singular visual portal; this is often done by shaping and victimization metaphysics and alternative reasoning to make sure ability at the appliance layer among several LBS service suppliers. Experimental results show the effectiveness of the systems.

REFERENCES

[1] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "Sybil Limit: A Near-Optimal Social Network Defense against Sybil Attacks," IEEE/ACM Trans. Networking, vol. 18, no. 3, pp. 885-898, June 2010.

[2] H. Hacig€um€us, S. Mehrotra, and B. Iyer, "Providing Database as a Service," Proc. IEEE 18th Int'l Conf. Data Eng. (ICDE), Feb. 2002.

[3] W.-S. Ku, L. Hu, C. Shahabi, and H. Wang, "Query Integrity Assurance of Location-Based Services Accessing Outsourced Spatial Databases," Proc. Int'l Symp. Advances in Spatial and Temporal Databases, July 2009.

[4] H. Hacig€um€u¸s, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service Provider Model," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD'02), pp. 216-227, 2002.

[5] B. Hore, S. Mehrotra, and G. Tsudik, "A Privacy-Preserving Index for Range Queries," Proc. 30th Int'l Conf. Very Large Data Bases (VLDB'04), pp. 720-731, Aug. 2004.

[6] B. Hore, S. Mehrotra, M. Canim, and M. Kantarcioglu, "Secure Multidimensional Range Queries over Outsourced Data," TheVLDB J., vol. 21, no. 3, pp. 333-358, 2012.

[7] E. Shi, J. Bethencourt, H. Chan, D. Song, and A. Perrig, "Multi-Dimensional Range Query over Encrypted Data," Proc. IEEE Symp. Security and Privacy (S&P'07), pp. 350-364, May 2007.

[8] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data, Proc. IEEE 30th Int'l Conf. Distributed Computing Systems (ICDCS'11), June 2011.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data, "Proc. IEEE INFOCOM, Apr. 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Access Control in Cloud Computing," Proc. IEEE INFOCOM'10, Mar. 2010.

[11] H. Pang and K.-L. Tan, "Verifying Completeness of Relational Query Answers from Online Servers," ACM Trans. Information and System Security, vol. 11, no. 2, pp. 1-50, Mar. 2008.

[12] M. Narasimha and G. Tsudik, "Authentication of Outsourced Databases Using Signature Aggregation and Chaining," Proc. 11thInt'l Conf. Database Systems for Advanced Applications (DASFAA'06), pp. 420-436, Apr. 2006

[13] H. Pang, J. Zhang, and K. Mouratidis, "Scalable Verification for Outsourced Dynamic Databases," Proc. VLDB Endowment, vol. 2, no. 1, pp. 802-813, 2009.

[14] Y. Yang, S. Papadopoulos, D. Papadias, and G. Kollios, "Spatial Outsourcing for Location-Mased Services," Proc. IEEE 24th Int'l Conf. Data Eng. (ICDE), pp. 1082-1091, Apr. 2008.

[15] M. Yiu, Y. Lin, and K. Mouratidis, "Efficient Verification of Shortest Path Search via Authenticated Hints," Proc. IEEE 26th Int'l Conf. Data Eng. (ICDE), pp. 237-248, Mar. 2010.

[16] M. Yiu, E. Lo, and D. Yung, "Authentication of Moving kNN Queries," Proc. IEEE 27th Int'l Conf. Data Eng. (ICDE), pp. 565-576, Apr. 2011.

[17] R. Merkle, "A Certified Digital Signature," Proc. Ninth Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 218-238, Aug. 1989.

[18] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Sensor Networks," Proc. IEEE INFOCOM'08, pp. 46-50, Apr. 2008.
[19] J. Shi, R. Zhang, and Y. Zhang, "Secure Range Queries in Tiered Sensor Networks," Proc. IEEE INFOCOM'09, Apr. 2009.
[20] R. Zhang, J. Shi, and Y. Zhang, "Secure Multidimensional Range Queries in Sensor Networks," Proc. ACM MobiHoc'09, pp. 197-206, May 2009.
[21] F. Chen and A. Liu, "Safe Q: Secure and Efficient Query Processing in Sensor Networks," Proc. IEEE INFOCOM'10, pp. 1-9, Mar. 2010.
[22] R. Zhang, J. Shi, Y. Liu, and Y. Zhang, "Verifiable Fine-Grained Top-K Queries in Tiered Sensor Networks," Proc. IEEE INFOCOM'10, Mar. 2010.

AUTHOR PROFILE

PITHANI SATYA SAMEERA ,is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Computer Science). Her Area of interest includes Secure Computing and its objectives in all current trends and techniques in Computer Science.

NALLI SUJATHA KUMARI **M.TECH** is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.