International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November2016

Detection of Untrusted Location Based Service providers Using Secure Spatial Top k Query Processing

D. Sukanya1 ,Ch. Sandeep2
PG Scholar, Dept of CSE, SR Engineering College, Ananthasagar, Warangal, TS, India.
Associate Professor, Dept of CSE, SR Engineering College, Ananthasagar, Warangal, TS, India.

Abstract: Storage nodes are predictable to be located as an intermediate tier of huge scale sensor networks for caching the composed sensor readings and responding to queries with reimbursements of impact and storage reduction for standard sensors. Nevertheless, an essential issue is that the compromised storage node may not only source the privacy problem, but also arrival fake/shortened query results. We propose a smooth yet skilled fake reading based anonymization constitution, beneath which the query result commitment can be certain by our proposed verifiable top-k query (VQ) schemes. Compared with accessible machinery, the VQ schemes have a essentially different design attitude and realize the lower communication complexity at the cost of slight exposure capability degradation. Analytical studies, geometric simulations, and archetype implementations are conducted to exhibit the practicality of our proposed methods.

Keywords-Sensor networks; Top-k query result completeness; VQ scheme.

I. INTRODUCTION

The flourish of smart phones contributes prosperity to location based services (LBSs) in nearly all social and business sectors, such as geo-social networks, merchandizing, marketing, and logistics. As these LBSs cause new business opportunities, there is a developing need of the mobile users to affirm the legitimacy of service results, such as a heeling of recommended local restaurants grouped by location and user rating. This moment is even more critical in an outsourced model where businesses (or data owners) publish their data to a 3rdparty service provider (SP), who handles LBS queries based on these data. As the SP is supposed to spoof query consequences in grace of their "sponsors", to sustain growth among fierce competition, it will soon be compelled to provide exploiters not only the effects, but also the proof of rightness. The data owner publishes not only data (e.g., spatial objects) to the SP, but also the endorsements of the data establishing exposed. These endorsements are signed by the data possess or fiddling with by the SP. Given a query, the SP brings back both the query results and a proof, named verification object (VO).

The VO is used by the verification phase, to rebuild the endorsements and thus assert the rightness of the results. However, one key restriction of all these works is that throughout the verification phase, the client is presumed to be completely hoped and ennobled to receive any data values, even though they are not part of the consequences. Unfortunately, this presumption is flawed in LBSs whose data is often sensitive locations and ought to remain secret against the client. For example, in online real-estate sites, the address of an attribute is often suppressed as business confidentiality. There is a call for privacy-preserving query authentication proficiencies in LBSs that assure the confidentiality of location data against the client. There is also a proposed privacy-preserving authentication for location-based wander queries. A location-based advertisement and recommendation are often recognized as one of the most productive LBS businesses and thus provoke the greatest controversy with their ranking results, here it is examined the privacy-preserving authentication for location-based top-k queries, where the rank assess of an object is a linear compounding of distance penalty and non-spatial score (e.g., user average rating). This query resolution is like to an abstraction of several location based top k queries defined in [11, 29] and even the k-nearest neighbour (kNN) queries. The first improvement say of image privacy-preserving

location-based top-k queries is its security framework. The effects of a top-k query imply the relative ranking of various objects. To address this, a formal security model founded on the computational is introduced. Second, the major cryptographic challenge of this problem is comparing the rank values of 2 objects without disclosing their locations or scores.

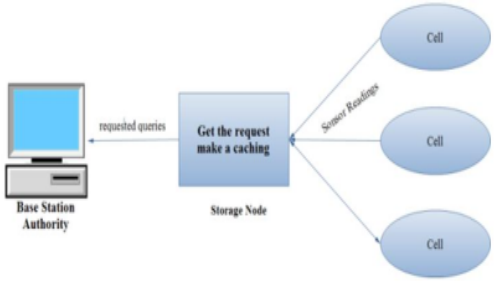
II. RELATED WORKS

Our work is most related to data outsourcing [4], for which we can only review representative schemes due to space constraints. The framework of data outsourcing was first introduced in [4], in which a data owner outsources its data to a third-party service provider who is responsible for answering the data queries from either the data owner or other users. In general, there are two security concerns in data outsourcing: data privacy and query integrity [5]. Ensuring data privacy requires the data owner to outsource encrypted data to the service provider, and efficient techniques are needed to support querying encrypted data.A bucketization approach was proposed in [6], [7] to enable efficient range queries over encrypted data, which was recently improved in [8]. Shietal. presented novel methods for multi-dimensional range queries over encrypted data[9]. Some most recent proposals aim at secure ranked keyword search [10], [11] or fine-grained access control [12]over encrypted data. This line of work is orthogonal to our work, as we focus on publicly accessible location-based data without need for privacy protection. Another line of research has been devoted to ensuring query integrity, i.e., that a query result is indeed generated from the outsourced data (the authenticity requirement)and contains all the data satisfying the query (the correctness requirement). In these schemes, the data owner outsources both its data and also its signatures over the data to the service provider which returns both the query result and verification object (VO) computed from the signatures for the querying user to verify query integrity. Many techniques were proposed for signature and VO generations, such as those [13], [14], [15]based on signature chaining and those [5], [16], [17], [18] based on the Merkle hash tree [19]or its variants. None of these schemes consider spatial top-k queries and are directly applicable to our intended scenario, as spatial top-k queries exhibit unique feature in that whether a POI is among the top-k is jointly determined by all the other POIs in the query region and that the query region cannot be predicted in practice. Secure remote query processing in tiered sensor networks[20], [21], [22], 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] to ensure data privacy against master nodes and also enable the network owner to verify range-query integrity. Moreover, Zhang et al. proposed efficient techniques for the network owner to validate the integrity of top-k queries.

III. THE PROPOSED APPROACH

A. System Architecture

Sensor reading gathered to the mobile. Group of sensor collection is known as cell. Each mobile gathering the some no of sensing data and in addition include the mobilephone. And then responding to queries with advantages of have an effect on and storage reduction for common place sensors. Here we use some algorithm encrypting the data after which approved signature additionally used on this section and then sends to the storage node. The storage node manner it's used to collect the sensing data's after which affirm the signature. The signature is tested approach it"s send with the aid of approved character. It is saved in storage node or not saved in storage node. And then ship to the base station or server to the sensing data right here we determine the digest values right or not and we going to decrypted the data. And determine that is common data or now not. The data is fashioned way we keep the records.



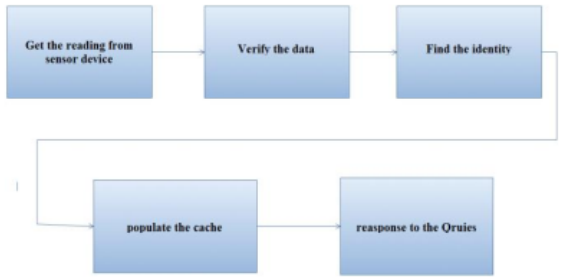
B. Preliminaries

i. Middle tier storage node access:

 The purpose of Middle tier to caching the sensed data for data archival and query response becomes necessary.

 It's performs the authority can issue queries to retrieve the sensor readings. The focal point tier is serene of a small number of storage-abundant nodes (storage nodes).

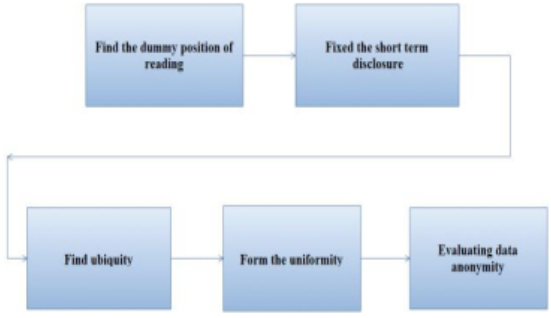
 The storage node is contains the copy of gathered sensor readings.



ii. Evaluating Data Anonymity:

 The anonymization having a many notions and they are similar but not same as each to other.

 We use statistical databases as means to maximize the query accuracy and minimize the probability of identifying meaningful individual records.



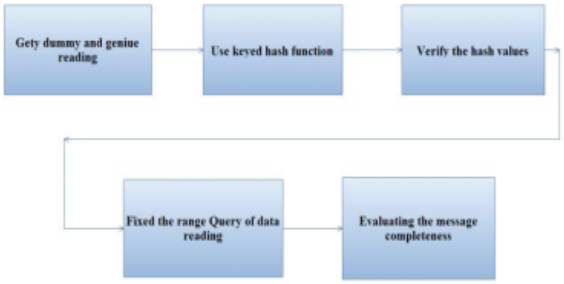
iii. Authentication for false injected reading:

 The dummy readings are generated randomly from they could collide with the legitimate cipher text that does not sense the corresponding reading. Without particular treatments, this kind of collision makes accept false readings. The authority should recover the genuine query result.

iv. Result verification:

 The AD Static scheme can solve the problem for data integrity and it check the hash value for identifying the top-k query variation.

 The result verification use the efficient performance in a low complexity.



C. Algorithm/Method Specification

1) The rdOPE Scheme Motivation: OPE has been applied widely to encrypted database salvage. Regrettably, in the prose, the data are all assumed to be generated and encrypted by a single authority, which is not the case in our deliberation. In toting up, since the quantity of do able sensor readings could be limited and known from hardware specification, the relation between plain texts and cipher texts could be revealed.

For example, if the sensors can only generate 20 kinds of possible outputs, then practically the adversary can derive the OPE key by investigating the numerical order of the eavesdropped cipher texts despite the theoretical security guarantee.

2) Algorithmic Description of rdOPE: Our solution is a novel use of OPE, called rdOPE, which provides the randomness in the encryption outputs and is suitable for the case of distributed data generation with limited input value range. The technical challenge of rdOPE design isto maintain the numerical orders of encryptions from different sensors that use different OPEs. With the observation that the possible mapping between plaintexts and cipher texts are fixed by A in advance, the cipher

texts can be determined prior to sensor deployment such that the numerical orders of ciphertexts in different sensors can be preserved. Two achievable concerns of implementing rdOPE on sensor networks are:

• the additional computation burden for A to calculate the rdOPE table, and

• the additional space requirement for each sensor to store the corresponding rows of the rdOPE table. B. The GD-VQ Scheme.

Basic Idea of GD-VQ The basic idea of GD-VQ is that the privacy, legitimacy, and completeness are cast iron by rdOPE, cryptographic hash, and the insertion of dummy readings, respectively. In particular, once the adversary cannot distinguish between genuine and dummy readings, the malicious removal of query results may cause the loss of dummy readings that are supposed to be included in the query result.

IV. CONCLUSION

A novel pretend reading-based anonymization framework is proposed to design Verifiable top- k Query (VQ) schemes. Inpicky, AD-VQ-static achieves the inferior‟s communiqué complexity with only slight detection ability consequence,which might be of both speculative and down-to-earth interests. Go together with by only symmetric cryptography implicated and their low realization obscurity, the VQschemes are apposite and sensible for current sensor networks.

REFERENCES

[1] Chia-Mu Yu, Chun-Shien Lu, and Sy-Yen Kuo§" Secure Multidimensional Queries in Tiered Sensor Networks" Taipei, [cs.NI] 16 dec 2009.

[2] Yi Dou, Jiutian Chen, Juan Feng, and Xiaolin Qin “Secure Query in Wireless Sensor Network Using Under ground Parties" vol 7, No. 12, dec 2012.

[3] Xiaojing Liao, Jianzhong Li “Privacy-preserving and Secure Top-k Query in Two-tier Wireless Sensor Network"

[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, May2007.

[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 CloudData,”Proc. IEEE INFOCOM, Apr. 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure,Scalable,and Fine-Grained Access Control in CloudComputing,” Proc.IEEE INFOCOM’10, Mar. 2010.

[11] H. Pang and K.-L. Tan, “Verifying Completeness of RelationalQuery Answers from Online Servers,” ACM Trans.Information andSystem 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'lConf. 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. IEEE26th 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.Electron.

[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. ACMMobiHoc'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.