Survey on Sheltered Top-K Query to Intermittently Encrypted Signature in Tiered Sensor Networks

P. Ramya 1, Dr. C. Nalini 2
Department of Computer Science & Engineering, Bharath University, Chennai, Tamil Nadu, 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 benefits of influence 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/curtailed query results. We propose a graceful yet competent dummy reading based anonymization constitution, beneath which the query result steadfastness 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

A. Motivation of the Project

To motivate effective dummy reading based anonymization framework, under which the query result integrity achieve the lower communication complexity at the cost detection. OPE has been applied widely to encrypted catalog reclamation. Regrettably, in the literature, the information is all assumed to be generated and encrypted by a single authority, which is not the case in our consideration. In addition, because the number of possible sensor Readings could be limited and known from hardware specification, the relation between plaintexts and cipher texts might be exposed. For example, if the sensors can solitary spawn 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.

B. Overview of the Project

The genuine top-k results are distributed to several sensor nodes. Through assured prospect, the influence
will find query result incompleteness by checking the other sensor nodes’ sensor readings. Amalgam routine is a collective use of supplementary facts and crosscheck, attempting to equilibrate the communiqué cost and the query result incompleteness detection capability. Top-k query result integrity was also addressed in where distributed data sources generate and forward the sensed data to a proxy node.

The query result completeness is achieved by requiring sensors to send cryptographic one-way hashes to the storage node even when they do not have fulfilling readings. In SMQ apiece sensor applies muddle operation to the received data and its hold data, generating a certifiable entity of the sensor readings of the entire network. The basic idea behind SMQ is to construct an aggregation tree over the sensor nodes.

The bucket index used in SMQ [34] leaks the possible value range for each sensor reading, which could be valuable information, to the adversary. Order Preserving Encryption (OPE), randomized and distributed OPE (rdOPE), is first developed to establish the privacy guarantee in the proposed Verifiable top-k Query (VQ) schemes. Our study evolves in a number of successive steps; we present Global Dummy reading-based VQ (GDVQ) and Local Dummy reading based VQ (LD-VQ), which constitute the foundation of our proposed dummy reading-based anonymization skeleton. Subsequently, they are superior to be Advanced Dummy reading-based VQ (AD-VQ), which reduces the communication overhead significantly.

C. Related Works

In this Paper [1] proposes on the Secure Range Query(SQR), Secure Top-k Query(STQ) and Secure Skyline Query(SSQ) schemes, developed at National Taiwan University, the outlooks covers the following like the Performance metrics, detection probability and communication cost and it concludes with the resiliency schemes against these two attacks. In this Paper [2] proposes the concept of secure multi-party in Internet of things or sensor networks making use of “underground parties” to guarantee network security, University of Posts and Telecommunications, it compares the time efficiency of the proposed algorithm with other typical sort algorithms under different top-k scenarios. Concludes homomorphic privacy and secure multi-party computation techniques. In this Paper [3] proposes the basic PriSec Topk scheme by using order-preserving encryption, developed at Harbin Institute of Technology, conclude that analysis investigating privacy, detection rate and efficiency guarantee and experiments on the real-world dataset. In this Paper [4] propose beneficial techniques to save power consumption and memory space consumption and buildup efficient query processing, technique named SafeQ, developed at Alagappa University, Merkle hash tree and neighborhood chain, reduce communication cost on sensor network. In this, Paper [5] surveys on series of collusion-aware privacy-preserving range query protocols in two-tiered WSNs, preservation of privacy and integrity, developed at Renmin University of China, in terms of efficiency, accuracy and privacy such as top-k and kNN, in two-tiered WSNs. In this Paper [6] proposes a simple yet effective dummy reading-based anonymization framework, verifiable top-k query (VQ) schemes. Analytical studies, numerical simulations, and prototype implementations are conducted to demonstrate conclude their low implementation difficulty. In this Paper [7] proposed schemes are build upon symmetric cryptographic primitives and force compromised master nodes to return both authentic and complete top-k query results to avoid being caught, confirm the high efficacy and efficiency, developed at New Jersey Institute of Technology, is most suitable for infrequent top-k queries with small query regions and more preferable with frequent top-k queries with large query regions. In this Paper[8] survey on investigate the secure co-operative data storage and query processing in UTSN, epoch schemes are generating an authentication and data confidentiality, developed at VTU, East west Institute of Technology, reduction in the delay, efficient query results evolution with low cost and multidimensional range queries, specific efficient enhancing steps for this scheme. In this Paper [9] proposes on novel distributed system for collaborative, location-based service providers (LBSPs) data collector about points-of-interest (POIs) LBSPs are untrusted and may return fake query results and effort to foster. Developed at Arizona State University, our schemes can enable users to verify the authenticity and correctness of any location-based top-k query results. The efficacy and efficiency of our schemes are thoroughly analyzed and evaluated through detailed simulation. In this Paper [10] survey on the explosive growth of Internet-capable and location-aware mobile devices, data contributors and perform spatial
top-k queries certain region with highest k ratings and detect fake spatial moving top-k query results. Conclude the efficacy and efficiency of our schemes are thoroughly analyzed and evaluated through detailed simulation studies.

<table>
<thead>
<tr>
<th>NAME OF THE PAPER</th>
<th>AUTHOR</th>
<th>PROBLEM ISSUE</th>
<th>TECHNIQUE IN EXISTING</th>
<th>EXISTING SYSTEM COMPARISION</th>
<th>PROPOSED ADVANTAGE</th>
<th>TOOLS/TECHNIQUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Multidimensional Queries in Tiered Sensor Networks</td>
<td>Chia-Mu Yu‡§, Chun-Shien Lu‡, and Sy-Yen Ku‡</td>
<td>securing range query, top-queries, and skyline query in tiered sensor networks</td>
<td>lowest communication overhead among prior works</td>
<td>Performance metrics, detection probability and communication cost</td>
<td>novel technique</td>
<td></td>
</tr>
<tr>
<td>Secure Query in Wireless Sensor Network Using Underground Parties</td>
<td>Haiping Huang,Yi Rui Zhang, and Xialin Qin</td>
<td>underground party nodes technique</td>
<td>misjudgment in seeking underground party nodes,</td>
<td>solves security and privacy-preserving query problems</td>
<td>horizontal and vertical query</td>
<td></td>
</tr>
<tr>
<td>Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks</td>
<td>Dr.V.Palanisamy MCA., M.Tech., #1, D.Gandhimathi</td>
<td>handling privacy</td>
<td>two tiered sensor network</td>
<td>Privacy and Integrity Preserving Range Query problem in sensor networks</td>
<td>Event driven sensor networks is achieved</td>
<td>SafeQ.</td>
</tr>
<tr>
<td>Collision-Aware Privacy-Preserving Range Query in Tiered Wireless Sensor Networks †</td>
<td>Xiaoying Zhang, Lei Dong, Hui Peng, Hong Chen ‡, Suyun Zhao and Cuiping Li</td>
<td>privacy of data and queries</td>
<td>privacy-preserving range query</td>
<td>increase in preserving</td>
<td>widespread adoption of WSNs and even threaten the security of the IoT</td>
<td></td>
</tr>
<tr>
<td>Top-k Query Result Completeness Verification in Tiered Sensor Networks</td>
<td>Chia-Mu Yu, Guo-Kai Ni, Ing-Yi Chen, Erol Gelenbe, Life Fellow, IEEE, and Sy-Yen Kuo, Fellow, IEEE</td>
<td>Storage nodes in large scale networks</td>
<td>VQ schemes</td>
<td>small scale networks</td>
<td>efficiency increased</td>
<td>dummy reading-based anonymization framework</td>
</tr>
<tr>
<td>Verifiable Fine-Grained Top-k Queries in Tiered Sensor Networks</td>
<td>Rui Zhang, Jing Shi, Yunzhong Liu, and Yanchao Zhang</td>
<td>nodes at the lower layer</td>
<td>symmetric cryptographic primitives</td>
<td>efficiency increased</td>
<td>high power in sensor nodes</td>
<td>Topk</td>
</tr>
<tr>
<td>A Survey On An Epoch Based Secure Data Aggregation And Authentication Scheme For Range Query Result Evaluation</td>
<td>Guruprasad Prasannag Dr. Arun Biradar</td>
<td>Incomplete query results may also occur due to leakage of data</td>
<td>multidimensional range queries</td>
<td>Capability increased</td>
<td>owner to master nodes for data confidentiality and completeness of the query</td>
<td>epoch schemes</td>
</tr>
<tr>
<td>Secure Top-k Query Processing via Untrusted Location-based Service Providers</td>
<td>Rui Zhang and Yanchao Zhang,Chi Zhang</td>
<td>distributed system for collaborative location-based information generation</td>
<td>poi,lbp’s</td>
<td>service increased</td>
<td>efficiency increased</td>
<td>novel schemes for users to detect fake top-k query</td>
</tr>
<tr>
<td>Secure Spatial Top-k Query Processing via Untrusted Location-based Service Providers</td>
<td>Rui Zhang,Jinchao Sun, Yanchao Zhang,Chi Zhang</td>
<td>Internet-capable and location-aware mobile devices</td>
<td>lpb’s,poi</td>
<td>security increased</td>
<td>efficiency increased</td>
<td>applying novel schemes</td>
</tr>
</tbody>
</table>
II. METHODS AND MATERIAL

A. System Architecture

Sensor reading collected to the cell. Group of sensor collection is called cell. Each cell collecting the some no of sensing data and also include the cell. And then responding to queries with benefits of influence and storage reduction for standard sensors. Here we use some algorithm encrypting the data and then authorized signature also used in this part and then sends to the storage node. The storage node means it’s used to collect the sensing data’s and then verify the signature. The signature is verified means it’s send by authorized person. It is stored in storage node or not stored in storage node. And then send to the base station or server to the sensing data here we check the digest values correct or not and we going to decrypted the data. And check this is original data or not. The data is original means we save the records.

B. Preliminaries

Modules
- Middle tier storage node access
- Evaluating Data Anonymity
- Authentication for false injected reading
- Result verification

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 doable sensor readings could be limited and known from hardware specification, the relation between plaintexts 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 is to 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 cipher texts 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.

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.

III. RESULTS AND DISCUSSION

This work implement by using java swing as a front end and my sql is backend.

Fig (a)

Fig (b)

Fig (c)

Fig (d)
which might be of both speculative and down-to-earth interests. Accompanied by only symmetric cryptography implicated and their low realization obscurity, the VQ schemes are apposite and sensible for current sensor networks..

V. REFERENCES


IV. CONCLUSION

A novel dummy reading-based anonymization framework is proposed to design Verifiable top-k Query (VQ) schemes. In picky, AD-VQ-static achieves the inferior’s communiqué complexity with only minor detection aptitude consequence,