© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

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

In sensor networks for records compilation, while there might be unhinged correlation between the authority (and network proprietor) and association, a core tier with the rationale of caching the sensed data for data archival and query response becomes necessary. The network model of this paper is illustrated where the authority can issue queries to retrieve the sensor readings. The core tier is serene of a petite number of storage-abundant nodes, called storage nodes. The bottom tier consists of a large number of resource-constrained ordinary sensors that sense the atmosphere. In the beyond tiered architecture, sensor nodes are usually partitioned into disjoint groups, each of which is associated with a cargo space node. Each group of sensor nodes is called a cell. The sensor nodes in a cell form a multi-hop network and always forward the sensor readings to the associated storage node. The storage node keeps a facsimile of customary sensor readings and is responsible for answering the queries from the authority.

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 equilibrium 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 (GD-VQ) 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

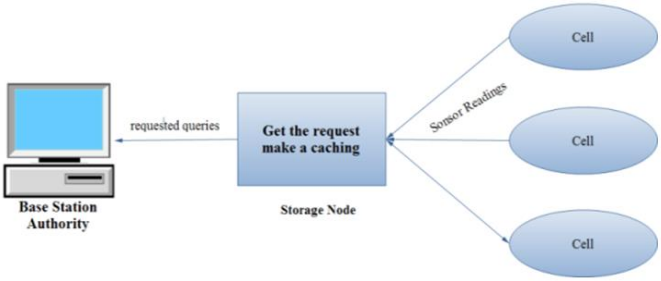
In this **Paper [1]** proposes on the Secure Range Query(SQR), Secure Top-k Query(STQ) and Secure Skyline Query(SSQ) schemes, developed at National Taiwan University, the outlooks covers the following like the Performance metrics, detection probability and communication cost and it concludes with the 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.

NAME OF THE PAPER	AUTHOR	PROBLEM ISSUE	TECHINQUE IN EXISTING	EXISTING SYSTEM COMPARISION	PROPOSED ADVANTAGE	TOOLS/TECNIQUE
Secure Multidimensional Queries in Tiered Sensor Networks	Chia-Mu Yu†§, Chun-Shien Lu†, and Sy-Yen Kuo§	securing range query, top-kquery, and skyline query in tiered sensor networks		lowest communication overhead among prior works	Performance metrics, detection probability and communication cost	novel technique
Secure Query in Wireless Sensor Network Using Underground Parties	Haiping Huang,Yi Dou,Jiutian Chen,Juan Feng,Xiaolin Qin	secure query	underground party nodes techniuqe	misjudgment in seeking underground party nodes,	solves security and privacy-preserving query problems	horizontal and vertical query
Privacy-preserving and Secure Top-k Query in Two-tier Wireless Sensor Network	Privacy-preserving and Secure Top-k Query in Two-tier Wireless Sensor Network Xiaojing Liao , Jianzhong Li	Sensitive data as well as returning fake query result.	using of Sensor nodes	two-tier wireless sensor network	investigating privacy, detection rate and efficiency guarantee of proposed scheme is achieved	PriSecTopk schemes
Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks	Dr.V.Palanisamy MCA., M.Tech., P.hD., #1, D.Gandhimathi	handling privacy	two tiered sensor network	Privacy and Integrity Preserving Range Query problem in sensor networks	Event driven sensor networks is achieved	SafeQ.
Collusion-Aware Privacy-Preserving Range Query in Tiered Wireless Sensor Networks †	Xiaoying Zhang, Lei Dong, Hui Peng, Hong Chen *, Suyun Zhao and Cuiping Li	privacy of data and queries	privacy-preserving range query	increase in preserving	widespread adoption of WSNs and even threaten the security of the IoT	queries performed efficiently and correctly
Top-k Query Result Completeness Verification in Tiered Sensor Networks	Chia-Mu Yu, Guo-Kai Ni, Ing-Yi Chen, Erol Gelenbe, Life Fellow, IEEE, and Sy-Yen Kuo, Fellow, IEEE	Storage nodes in large scale networks	VQ schemes	small scale networks	efficiency increased	dummy readingbased anonymization framework
Verifiable Fine-Grained Top-k Queries in Tiered Sensor Networks	Rui Zhang, Jing Shi, Yunzhong Liu, and Yanchao Zhang	poor sensor nodes at the lower tier	symmetric cryptographic primitives	efficiency increased	high power in sensor nodes	Topk
A Survey On An Epoch Based Secure Data Aggregation And Authentication Scheme For Range Query Result Evaluation	Guruprasad Prasanna G Dr.Arun Biradar	Incomplete query results may also occur due to leakage of data	multidimensional range queries	*Capabliy increased*	owner to master nodes for data confidentiality and completeness of the query	epoch schemes
Secure Top-k Query Processing via Untrusted Location-based Service Providers	Rui Zhang and Yanchao Zhang,Chi Zhang	distributed system for collaborative location-based information generation	poi,lbsp's	service increased	efficiency increased	novel schemes for users to detect fake top-k query
Secure Spatial Top-k Query Processing via Untrusted Location-based Service Providers	Rui Zhang,Jinchao Sun,Yanchao Zhang,Chi Zhang	Internet-capable and location-aware mobile devices	lpb's,poi	security incresed	efficiency increased	applying novel schemes

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.

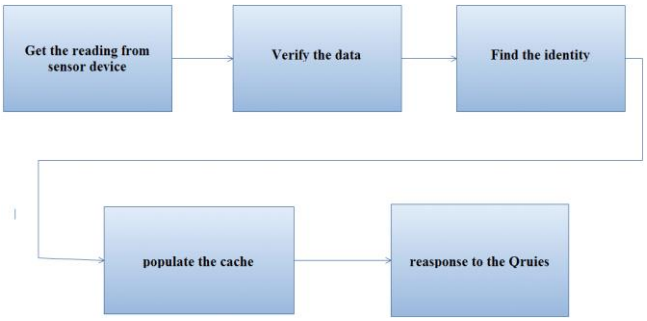
B. Preliminaries

Modules

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

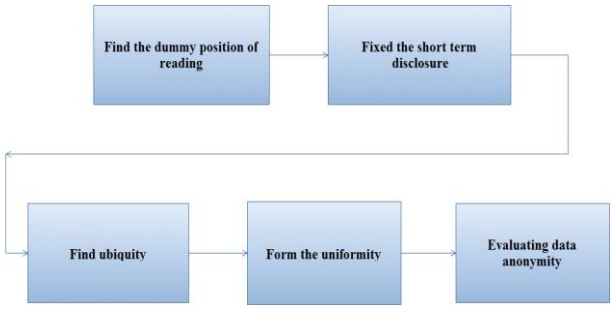
i. Middle tier storage node access:

- 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.



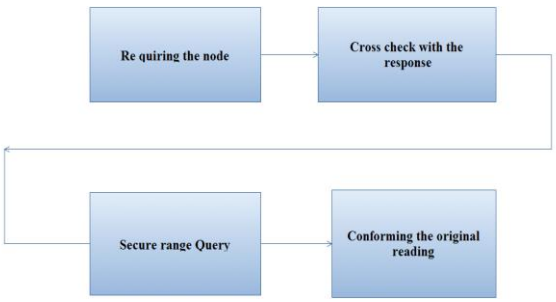
ii. Evaluating Data Anonymity:

- 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.



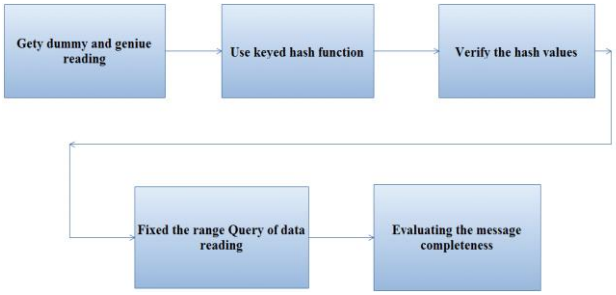
iii. Authentication for false injected reading:

- 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. 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.

III. RESULTS AND DISCUSSION

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

Fig (a)

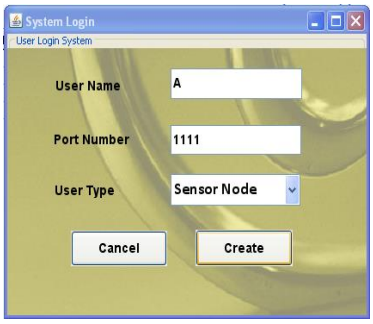
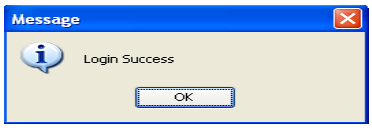


Fig (b)



Fig(c)

Fig (a) is system login. Fig (b) here we give the user name and port no and then select the user type and then click the create button. Fig (c) The login box can be apper in the desktop. Login successand click the ok butten.

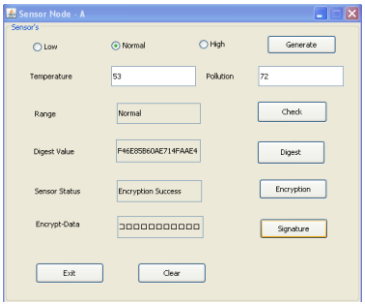


Fig (d)

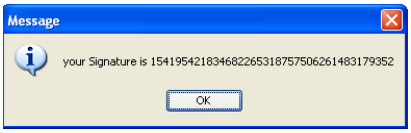


Fig (e)

Fig (d) is storage node here we select any one of the button and then click generate. The temperature and pollution will be appearing in the storage node. And then check the range then digest the value and encrypting and create a signature. Fig (e) signature create box.

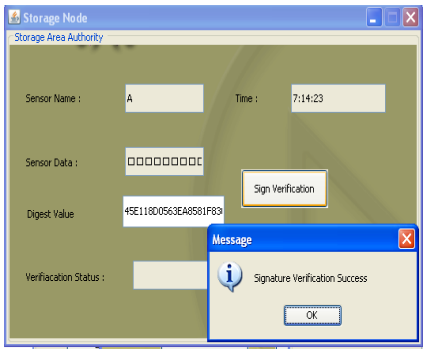


Fig (f)

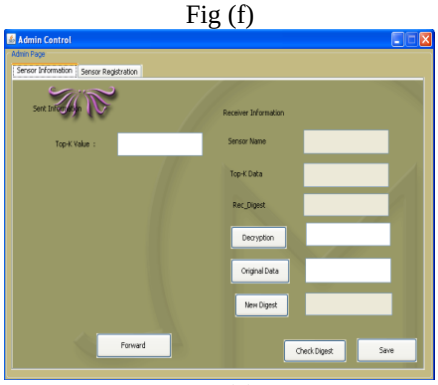


Fig (g)

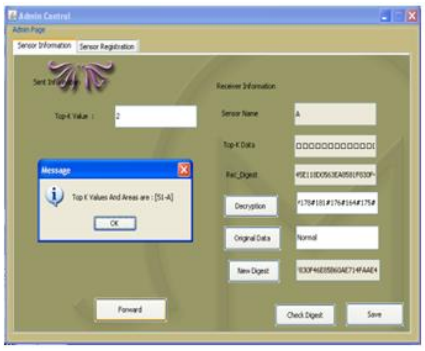


Fig (h)

Fig (f) is signature varification box. Fig (g) is admin control or server box. Fig (h) here we use decrypting the message and then check the results. The data is orinal means the record will be saved in the server.

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, 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

[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 Underground 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] Dr.V.Palanisamy MCA., M.Tech., P.hD., #1, D.Gandhimathi*2 "Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks" ijptt, vol.3, Issue 3, apr-2013.

[5] Xiaoying Zhang, Lei Dong, Hui Peng, Hong Chen *, Suyun Zhao and Cuiping Li," Collusion-Aware Privacy-Preserving Range Query in Tiered Wireless Sensor Networks" 2014, 14, 23905-23932.

[6] Yu, C., G. Ni, I. Chen, Erol Gelenbe, and S. Kuo. "Top-k Query Result Completeness Verification in Tiered Sensor Networks." (2014): 1-1.

[7] Rui Zhang, Jing Shi, Yunzhong Liu, and Yanchao Zhang, "Verifiable Fine-Grained Top-k Queries in Tiered Sensor Networks"

[8] Guruprasad, Prasanna G and Dr.Arun Biradar, "A Survey on an Epoch Based Secure Data Aggregation and Authentication Scheme for Range Query Result Evaluation" IJERT, vol. 2, Issue 3, march-2013.

[9] R. Zhang, Y. Zhang, and C. Zhang, "Secure top-k query processing via untrusted location-based service providers," inProc. 24th IEEE Conf. Comput. Commun., Mar. 2012, pp. 1170–1178.

[10] R. Zhang, Jinchao Sun, Y. Zhang, and C. Zhang," Secure Spatial Top-k Query processing via Untrusted Location-based Service Providers", 2013 IEEE.