ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Secure Top-*K* Query to Variably Encrypted Signature in Tiered Sensor Networks

P.Ramya, Dr.C. Nalini

PG Student, Dept. of C.S.E., Bharath University, Chennai, India

Professor, Dept. of C.S.E., Bharath University, Chennai, 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 an 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.

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.

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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.

II. RELATED WORK

A. Fast Privacy-Preserving Top-k Queries using Secret Sharing

Over the past several years a lot of research has focused on distributed top-k division. In this work we are fascinated in the next privacy-preserving distributed top-k quandary. A situate of parties grasp secretive lists of key-value pairs and want to find and disclose the k key-value pairs with largest aggregate values without revealing any further information. We use sheltered multiparty computation (MPC) techniques to solve this problem and design two MPC protocols, *PPTK* and *PPTKS*, putting prominence scheduled their effectiveness. *PPTK* uses a chop table to squeeze a probably large and sparse space of keys and to probabilistically estimate the aggregate values of the top-k keys. *PPTKS* uses manifold botch tables, i.e., sketches, to progress the inference precision of *PPTK*. We estimate our protocols with real interchange traces and show that they accurately and efficiently aggregate distributions of IP addresses and port numbers to find the globally most frequent IP addresses and port numbers [5].

B. Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks

Two tiered sensor network architecture, someplace storage nodes proceed as an intermediary tier between sensor nodes and sink which is act as a receiver for storing data items and calculating queries. I propose beneficial techniques to save power consumption and memory space consumption and buildup efficient query processing. For preserve privacy, I propose a technique named SafeQ. SafeQ is a protocol, which is used to detect misbehavior of attackers. And storage node can perfectly process queries issued from sink and data items sent by sensor nodes without knowing their inventive values. For care for veracity, I intend two methods namely Merkle hash tree and vicinity manacles. Mutually be used for corroborate whether the query result of data items that satisfy the query. For reduce communiqué cost, I propose flourish filters for diminish the communiqué cost between sensor nodes and storage nodes in sensor networks [6].

C. SafeQ: Secure and Efficient Query Processing in Sensor Networks

The architecture of two-tiered sensor networks, somewhere storage nodes give out as a transitional tier between sensors and a sink for storing data and doling out queries, has been extensively adopted since of the reimbursement of power and storage saving for sensors as well as the efficiency of query meting out. Conversely, the magnitude of storage nodes also makes them striking to attackers. In this paper, we intention SafeQ, a etiquette so as to prevents attackers on or after gaining information from both sensor collected data and sink issued queries. SafeQ too allows a fall to perceive compromised storage nodes when they act up. *To preserve privacy*, SafeQ uses a novel technique to encode both data and queries such that a storage node can correctly process encoded queries over

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

encoded data without knowing their ideals. *To preserve integrity*, we intend a novel data structure called neighborhood chains that allow a sink to verify whether the result of a query contains exactly the data items that gratify the query. In toting up, we intend a clarification to acclimatize SafeQ for event-driven sensor networks [7].

D. Top-k Monitoring in Wireless Sensor Networks

Top-k monitoring is important to many wireless sensor applications. This term paper exploits the semantics of top-k query and proposes an energy-efficient monitoring loom called FILA. The essential initiative is to establish a sieve at each sensor node to suppress unnecessary sensor updates. Sieve scenery and query reassessment in front updates are two fundamental issues to the correctness and efficiency of the FILA loom. We enlarge a query reassessment algorithm that is capable of handling concurrent sensor updates. In finicky, we turnout optimization techniques to shrink the prying cost. We devise a skewed sieve locale scheme, which aims to steadiness energy expenditure and prolong network existence. Besides, two sieves revise strategies, explicitly, fervent and sluggish, are anticipated to favor different relevance scenarios. We as well widen the algorithms to quite a few variants of top-k query, that is, classify numb, rough, and value monitoring. The performance of the proposed FILA approach is extensively evaluated using factual data traces. The consequences show that FILA significantly outperforms the existing TAG-based approach and range caching approach in terms of both network lifetime and energy consumption under various network configurations[8].

E. Secure Top-k Query Processing via Untrusted Location-based Service Providers

Distributed system for collaborative location-based information generation and sharing which become increasingly popular due to the explosive growth of Internet-capable and location-aware itinerant devices. The arrangement consists of a data aerial, data contributors, location-based overhaul providers (LBSPs), and system users. The data collector gathers reviews about points-of-interest (POls) from data contributors, whilst LBSPs acquire POI data sets as of the data collector and allow users to perform location-based top-k queries which ask for the POls in a certain region and with the highest k ratings for an interested POI trait. In carry out, LBSPs are untreated and can return fake query results for various bad motives, e.g., in favor of POls agreeable to pay. This dissertation presents two novel schemes meant for users to detect fake top-k query results as an effort to foster the practical deployment and use of the wished-for system. The effectiveness and good organization of our schemes are thoroughly analyzed and evaluated [9].

III. VERIFIABLE TOK-K QUERY SCHEME

In tiered sensor networks, the authority issues proper queries to retrieve the desired portion of sensed data. We restrict ourselves in this paper to discussing top-*k* query, which is one of the most intuitive and commonly used queries. Top-*k* query can be used to extract the extreme sensor readings. By intercepting the sensor infrastructure, the antagonist canister obtains the sensed data. By compromising storage nodes, the adversary can also return the falsely injected readings to the authority. The most challenging is that the compromised storage nodes can violate query result totality, creating a deficient query result intended for the authority by replacing some portions of the query result with the other genuine readings. The Verifiable top-*k* Query (VQ) schemes based on the novel dummy reading-based anonymization framework are proposed for privacy preserving top-*k* query result integrity verification in tiered sensor networks. A randomized and disseminated adaptation of Order Preserving Encryption, rdOPE, is wished-for to be the privacy institution. AD-VQ-static achieves the lower communication complexity at the cost of slight detection aptitude squalor, which could be of mutually speculative and practical interests. Storage nodes are storage-abundant, can converse with the influence *A* through direct or multi-hop interactions, and are implicit to know their allied cells. Instant on the nodes has been harmonized and is divided into epochs. With different types of data flow, two phases are considered by the first is *data submission phase*, during which the sensors submit the sensed data to the nearest associated storage node. At the end of each epoch, each sensor enters this phase. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

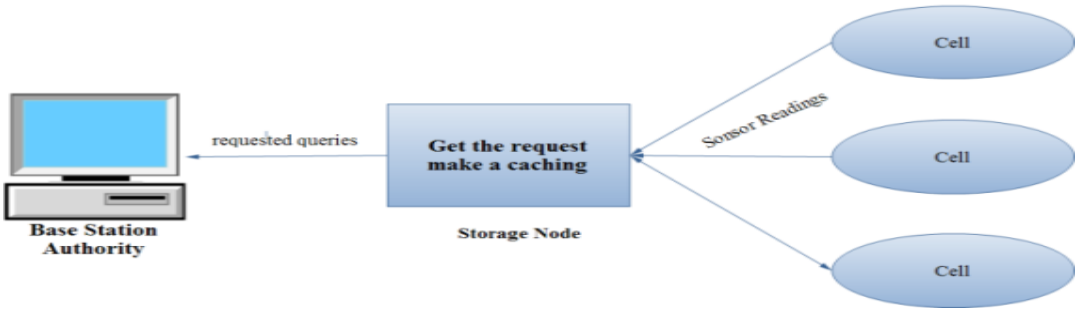
second is *query response phase*, during which the storage node responds to the query issued by *A*. We particularly note that the keyed hash functions used in this paper are keyed-hash message authentication code (HMAC). Consider two parties sharing a secret key *k*. If the message *m* to be communicated is associated with *HMACk (m)*, the use of HMAC naturally guarantees the data authenticity and integrity.

Performance metrics are used to evaluate the integrity verification methods for detection probability, communication cost.

Advantages:

The narrative dummy reading-based anonymization skeleton is proposed for privacy preserving top-*k* query result integrity verification in tiered sensor networks. A randomized and distributed version of Order Preserving Encryption, rdOPE, is wished-for to be the privacy foundation. AD-VQ-static achieves the lower communication complexity at the cost of slight detection capability degradation, which could be of both theoretical and practical interests.The keyed hash functions used in this paper are keyed-hash message authentication code (HMAC). The two parties sharing a secret key *k*. If the message *m* to be communicated is associated with *HMACk (m)*, the use of HMAC naturally guarantees the data authenticity and integrity.

IV. SYSTEM ARCHITECTURE



V. PRELIMINARIES

Modules

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

A. Middle tier storage node access:

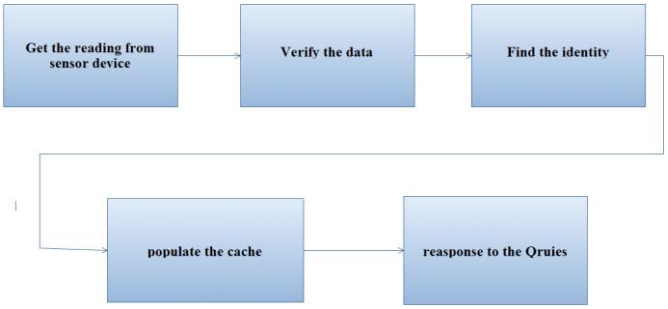
- The purpose of Middle tier to caching the sensed data for data archival and query response becomes necessary.
- It's performs the authority can issue queries to retrieve the sensor readings. The focal point tier is serene of a small number of storage-abundant nodes (storage nodes).
- The storage node is contains the copy of gathered sensor readings.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

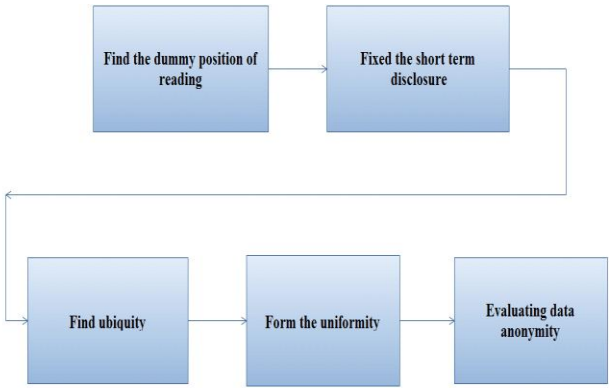
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015



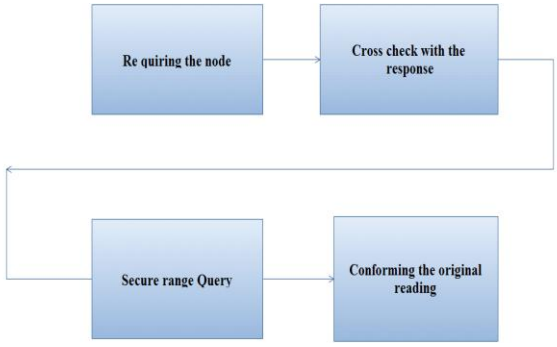
B. Evaluating Data Anonymity:

- 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.



C.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.



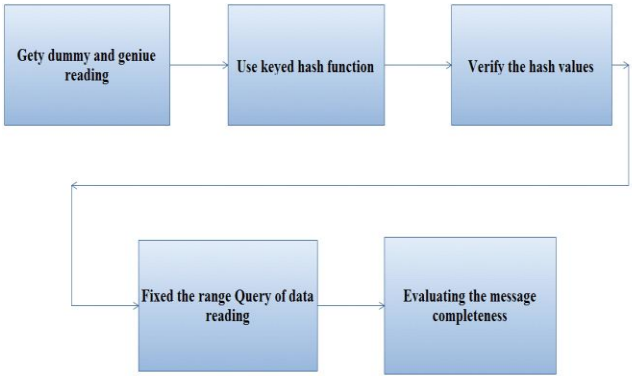
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

D. 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

VI. 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

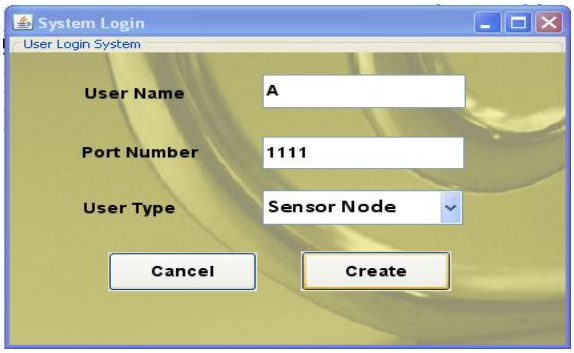
International Journal of Innovative Research in Computer and Communication Engineering

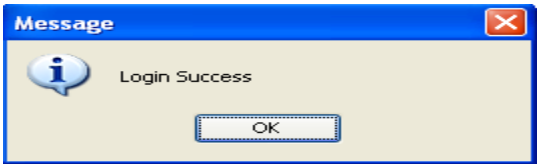
(An ISO 3297: 2007 Certified Organization)

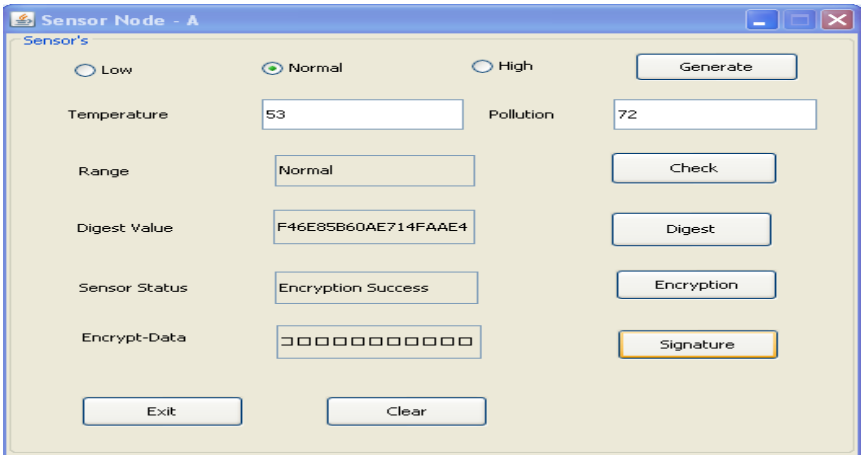
Vol. 3, Issue 3, March 2015

VII. EXPERIMENT SET OF RESULT

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





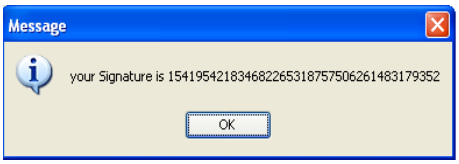


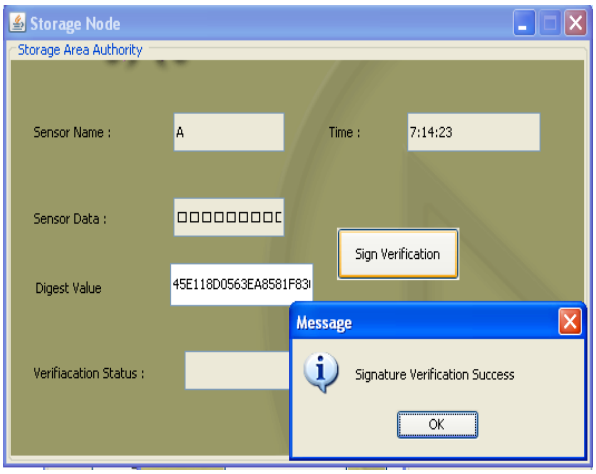
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

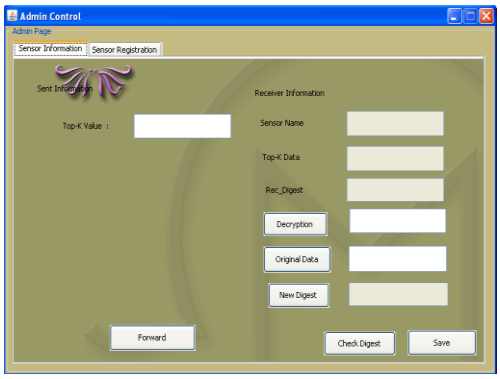
International Journal of Innovative Research in Computer and Communication Engineering

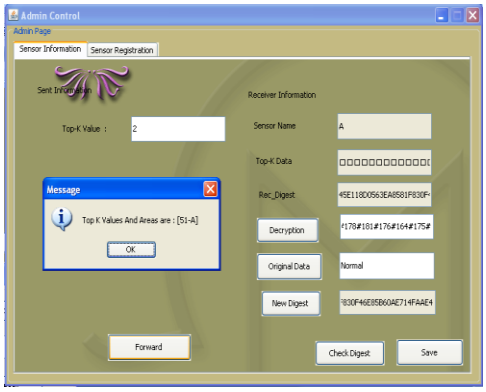
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015









VIII. 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 inferioSr 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.

REFERENCES

1. Yu, C., G. Ni, I. Chen, Erol Gelenbe, and S. Kuo. "Top-k Query Result Completeness Verification in Tiered Sensor Networks." (2014): 1-1.
2. E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," *Comput. Netw.*, vol. 51, no. 5, pp. 1299–1314, 2007.
3. Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. INFOCOM*, Apr. 2003, pp. 1976–1986.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

4. H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proc. ICPS*, Jul. 2005, pp. 88–97.
5. M. Burkhart and X. Dimitropoulos, "Fast privacy preserving top-k queries using secret sharing," in *Proc. 19th ICCCN*, 2010, pp. 1–7.
6. Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Privacy- and integrity-preserving range query in wireless sensor networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2012, pp. 328–334.
7. F. Chen and A. X. Liu, "SafeQ: Secure and efficient query processing in sensor networks," in *Proc. 24th IEEE Conf. Comput. Commun.*, Mar. 2010, pp. 1–9.
8. M. Wu, J. Xu, X. Tang, and W.-C. Lee, "Top-k monitoring in wireless sensor networks," *IEEE Trans. Knowl. Data Eng.*, vol. 19, no. 7, pp. 962–976, Jul. 2007.
9. R. Zhang, Y. Zhang, and C. Zhang, "Secure top-k query processing via untrusted location-based service providers," in *Proc. 24th IEEE Conf. Comput. Commun.*, Mar. 2012, pp. 1170–1178.