JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Top-k Query response Completeness evaluation and Verification in Tiered Sensor Networks

Appasani Keerthi[1] **Dr.R. Vasavi**[2]

ABSTRACT

A few wireless sensor applications require the most vital sensor data in the environment. In such applications, sensor nodes continuously transmit data to storage nodes for a set length of time. It oversees transmitting the obtained results to the Top-K rule that anticipates them. Dummy data was included in the original content material details to protect the information from enemies who compromised the sensor and storage nodes. If an attacker hacks the storage node, false information will be delivered to the command. Steganography has been integrated with an effective method known as add-up complete signature to establish the message's originality and safeguard the data against the most recent security threats. Before sending the information from the command to the storage nodes, an indexed-founded construct for the database record has also been provided to check the resources against availability.

1.INTRODUCTION

A core being straight with the reason of caching the sensed data for facts archive and inquiry reply becomes fair, even if there may be a skewed relationship between the authority (and contacts owner) and organization in sensor networks for records compilation. Where the connection technique of this essay is organized is where the regime can employ issue interrogation to retrieve the sensor readings. Storage nodes, or nodes with a lot of storage, make up much of the basic level. The lower level was created by several common detectors using meager resources to sense their environment. readings sent to the corresponding storage node. The storage node oversees responding to the authority's questions and maintains a replica of typical sensor readings. they ask for outcome integrity to achieve lower communication complexity at the tag detection and to motivate powerful dummy perusing founded anonymization architecture. The recuperation of encrypted catalogs has seen extensive use of OPE. Unfortunately, in literature, it is assumed that all the data was created and encrypted by a single entity; however, this is not the issue we are considering. In addition, the relationship between plaintext and cipher text is likely to be revealed because the range of possible sensor readings is perhaps constrained and is known from hardware specifications. Even though the theoretical security forbids it, the attacker can to some extent obtain the OPE key by examining the numerical bid of the eavesdropped cipher messages, for instance, if the detectors can alone generate 20 different types of possible outputs.

A few sensor nodes receive accurate top-k findings. By comparing the sensor readings from the other sensor nodes, the effects will most likely identify the effect's incompleteness. Combining additional information and cross-checks is known as an amalgam routine, and it aims to strike a balance between the question outcome incompleteness detection capabilities and the communiqué tag. The integrity of top k ask results was addressed in distributed information sources that create and communicate sensed information to a proxy node. The ask-execute completeness is achieved by requiring detectors to provide cryptographic one-way hashes to the storage node even when they do not have satisfying readings.

In SMQ, a sensor takes a jumbled approach to the received facts and its own data, producing a certifiable entity out of the sensor readings of the concluded connections. The key immodesty of SMQ is the generation of an aggregate tree over the sensor nodes. The bawdy index used in SMQ [34] discloses the possible value range for each sensor reading to the adversary, which could be critical information. While the rule in sensor networks may have an unbalanced connection for details compilation, a core being

straight with the objective of storing the felt facts for facts archival and inquiry answer becomes important. This article depicts the connecting device and explains how the rule can send requests to retrieve sensor readings.

The core level was created entirely of storage-rich nodes or storage nodes. The lowest level is made up of a slew of rudimentary detectors with limited resources that observe the environment. In an overhead-tiered architecture, sensor nodes are often divided into division groups.

To encourage the development of a strong dummy reading-based anonymization framework that reduces intercommunication complexity at the expense of detection. OPE is often used in encrypted catalog reclamation. Unfortunately, the details in the literature are all assumed to have been developed and encrypted by a single authority, which is not the case in our scenario. Furthermore, due to the large number of possible sensors, the relationship between plaintexts and cipher texts may be disclosed. Readings may be minute and derived from hardware specifications.

2. RELATED WORK

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

To encourage the development of a strong dummy reading-based anonymization framework that reduces intercommunication complexity at the expense of detection. OPE is often used in encrypted catalog reclamation. Unfortunately, the details in the literature are all assumed to have been developed and encrypted by a single authority, which is not the case in our scenario. Furthermore, due to the large number of possible sensors, the relationship between plaintexts and cipher texts may be disclosed. Readings may be minute and derived from hardware specifications.

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

An anonymization framework based on OPE attempts to reduce communication complexity and detection costs while maintaining integrity. Literature, on the other hand, suggests that information was invented and encrypted by a single nation. As the link between plaintext and cipher material is revealed, the quantity of sensor readings becomes vulnerable. I'd like to use two ways to ensure veracity: the Markel hash tree and proximity manacles. Corroborate if the inquiry result comprises information items that satisfy or please the inquiry. In sensor networks, I propose flourish filters to reduce the cost of intercommunication between sensor nodes and storage nodes.

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

On the other hand, storage nodes' importance also sets them apart from attackers. In this study, we create Safe, a protocol designed to prevent attackers from learning information from both sensor-gathered facts and sink-reissued questioning. Safe Q also enables autonomous observers to monitor problematic resolved storage nodes. Safe Q uses an inventive technique to encode data and questioning to maintain privacy, allowing a storage node to conduct encoded interrogation over encoded data without quickly changing their minds. We aim to apply a novel data composition called neighborhood chains, which enables a sink to authenticate if the outcome of an inquiry has precisely the information items necessary, to maintain integrity.

D. Top-k Monitoring in Wireless Sensor Networks.

Some wireless sensor applications require top observation. This phrase suggests an energy-efficient watching loom called FILA that takes advantage of the semantics of top k ask. To prevent pointless sensor updates, it is imperative to validate a sieve at each sensor node. Two major problems with the accuracy and effectiveness of the FILA loom are the sieve scenery and the request for reassessment in forward upgrades. We expand a system for question re-evaluation that can handle many sensor updates at once. We use cunning optimizing techniques to evade the nosy tag. We created a skewed sieve location design with the goal of regulating energy consumption and extending the lifespan of bonds.

Additionally, it is envisaged that two sieve techniques, expressly fervent and slow, will Favor clear relevance instances. We also extend the algorithmic programmer to several top inquiry options, i.e., write dull, rough, and interesting to watch. Using precise information traces, the effectiveness of the advised FILA progress is thoroughly assessed. According to the findings, FILA outperforms TAG-based and range caching advances in terms of call lifespan and power consumption for various call configurations.

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

Distributed draw enables cooperative location-based information gathering and sharing, which has gained popularity because of the rapid development of mobile gadgets with Internet access and location awareness. A data aerial, fact contributors, location-based

overhaul providers (LBSPs), and address consumers make up the arrangement. While LBSPs receive POI information sets from the data collector and enable users to direct location-based top-k interrogations that contemplate requesting the POIs in a specific area, the details collector gathers reviews regarding points-of-interest (polls) from fact contributors.

A trait that is alive to POI and has the greatest k ratings. In conclusion, LBSPs are untreated and have the potential to produce false search results for a variety of negative intentions, such as casting a vote for polls that offer reimbursement. To encourage the practical implementation and usage of the desired draw, this dissertation presents two cutting-edge strategies designed to help users uncover phony top-k ask outcomes. Our system's efficacy and solidity are carefully examined and assessed.

3. EXISTING WORKS ON DATA SECURITY

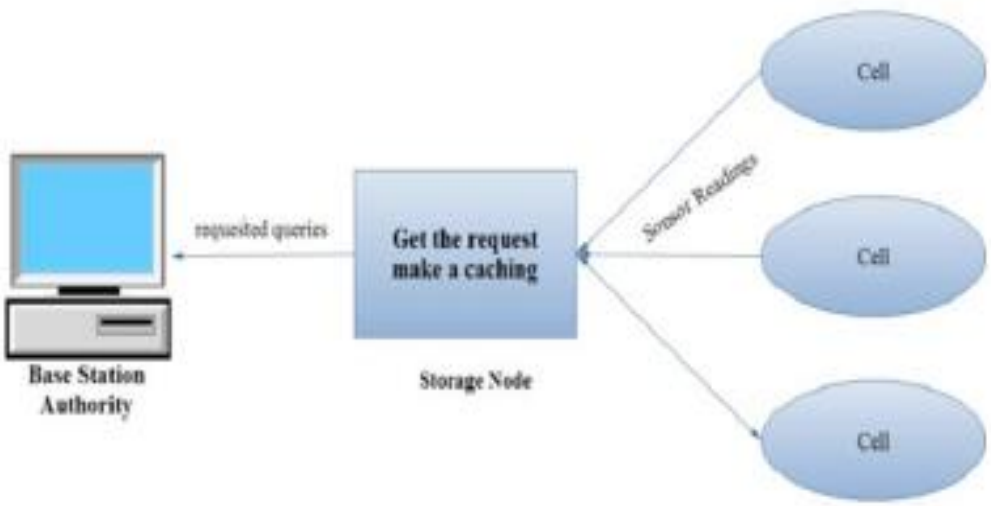
Many secure procedures must be used when moving information across the communication medium to protect it from an opponent. The standard technology used two methods to secure the data: extra proof and a repulsive check. Additional evidence [1] generates a message digest to confirm the specifics. The message will be read by the sender before being forwarded to the device. By comparing the freshly generated digest with the corresponding retrieved message and cross-referencing them, the handset oversees confirming the message digest.

It would be preferable if the adversary had changed the facts in the middle of the communication medium if there were any disputes. The information is distributed to the nearby sensor nodes using the cross-check technique [2]. The owner can verify the accuracy of the inquiry by contrasting the information it has obtained from the sensor node with similar information it has sought from another sensor node nearby. Combining overhead approaches results in a hybrid approach [6]. It is used to assess the validity and thoroughness of the investigation. The technology used by the verifiable ask processing method involves sending cryptographic one-way hashes.

Storage nodes, even when they do not have to fulfil or please readings big sensor networks have a two-tier architecture in which the sensor nodes report the information to the vanquished node, which then transmits the information to the ruling party. Due to the importance of the information, it has been crucial to secure the data in the two-tier design. Verifiable If the information is compromised by the attacker, the top-k ask mechanism [6] is put in place to find any inaccurate results given to the owner by the vanquished nodes. By embedding numerous linkages between the data elements, verification is carried out by the owners.

As a step forward in detecting sensor node settlement, the ask conversion construct has been made available, resulting in the communication of the irrelevant details to the conquered nodes. To find potential colluding assaults from settles detectors and vanquish nodes, random probing attracts have been included. By randomly comparing the effect among the nearby sensor nodes to check the validity of the effect, the owner confirms the information it obtained. By looking at the testimonies from observer nodes, a clever burden design called RW is used to determine the resolve of the sensor node. The owner can confirm the integrity and comprehensiveness of the data by using the overhead approaches.

4. SYSTEM ARCHITECTURE



VERIFIABLE TOK-K QUERY SCHEME

The command issue is a crucial inquiry in tiered sensor networks to obtain the desired component of sensed facts. As one of the easiest and most often used interrogations, we restrict our discussion in this article to top-k questions. It is possible to utilize top k ask to remove the surplus sensor readings. The competing canister acquires the sensed information by intercepting the sensor network. The adversary can also send the erroneously injected readings back to the command by infiltrating storage nodes. The most important is that the resolved storage nodes can fragment the totality of the query result, creating a defective query outcome intended for the government by substituting some of the query result's components with other real readings.

It is advised to use the Verifiable top-k ask (VQ) techniques for tiered sensor networks' top-k ask effect integrity verification since they are built on the ground-breaking dummy reading-based anonymization framework. As the privacy institution, rope, a randomized and distributed version of bid-maintaining encryption, is desired. Possibly both theoretically and practically, AD-VQ-static reduces communication complexity at the expense of a little deterioration in detecting aptitude. Storage nodes have a lot of storage, can communicate with several hops or overdriven interactions, and implicitly can grab their ally cells.

The nodes' instant has been epoch-segregated and harmonized. Two phases are taken into consideration when clear types of information flow: the facts submission phase, during which the detectors confirm the sensed information to the nearest corresponding storage node. Each sensor pierces this phase at the start of each epoch. The storage node responds to the ask made by A in the second phase, known as the ask response phase. The keyed-hash message authentication programming verbal communication (HMAC) hash functions utilized in this conclusion are noted specifically in the last section.

Consider two individuals who share a secret key. The application of HMAC ensures the truthfulness and integrity of the information if the message m to be conveyed is linked to H MAC (m). The integrity verification methods for detection likelihood and communication tag are evaluated using effectiveness measures.

4.1 ADVANTAGE:

For privacy, a narrative dummy reading-based anonymization skeleton is offered. In tiered sensor networks, however, the top-k ask result integrity verification comes next. The privacy foundation is desired to be a randomized and distributed system of privacy-conserving encryption, called rode. Theoretically and practically, AD VQ-static reduces communication complexity at the expense of a modest reduction in detecting capabilities. The keyed-hash message authentication programming verbal communication (HMAC) is the keyed-hash function utilized in this finance. A secret key is made known by the two parties. If H MAC (m) and the message m to be transmitted are linked, the application.

4.2 EFFICIENCY AND SECURITY GAP

However, despite the prior work, the following issues still need to be resolved: Communications with a hybrid arrangement [7] yield O(n2) rates. Large-scale networks are not appropriate applications for the Mote Sec-Aware construct [5]. Due to the shared encryption key between the leader and sensor nodes in KLM, the usage of symmetric cryptography is less effective. The neighboring Dominance

Graph [3], which handles continuous top-k queries, is intended to operate in a homogeneous setting. On receiving a request from a few clients for lookalike data, it is frequently necessary to do repeated high interrogations in the DB to retrieve information. If any one of the sensor nodes is settled, the adversary may easily find the symmetric key [6] shared by all the sensor nodes. The checking process at each.

4.3 AUTHORITY DATA VALIDATION PROCESS

The government oversees recovering the information embedded within a character using the necessary steganography decrypting procedures. Following the retrieval of the data, the information must be decrypted using asymmetric key encryption. To encrypt and decrypt the facts, the government and sensor nodes employ clear sets of keys. The message is encrypted with the sender's public key using asymmetric key encryption. No one will be able to decrypt the content because the owner will be the only one who can.

Having the private key allows you to decode the material. Because learning the key for decrypting the material is difficult, the adversary will never be able to crop the data. Because the message signed by the sender can only be viewed by the person who possesses the associated decrypting key, secrecy is preserved while employing the overhead approach. The owner will only share the decryption key with trusted persons.

The second level of assurance of facts has been ensured with the help of message digesting the information in an asymmetric key that the factual content sent by the sender is unmodified, which results in achieving the consequences of integrity and completeness while transferring the data in the communication medium. The regime is responsible for updating the associated sensor details in the database after decrypting the data. All information about the sensor's surroundings will be saved in the database, with each sensor ID having its own punch in the database.

5. ALGORITHM/METHOD SPECIFICATION

1) The rdOPE Scheme Motivation:

OPE has been widely used in the recovery of encrypted databases. Regrettably, the facts are all presumed to have been generated and encrypted by a single regime in the article; this is not the topic under consideration. To summarize, because the number of possible sensor readings is likely to be limited and known from hardware specifications, the relationship between plaintexts and cipher texts may be exposed. For example, if the detectors can only provide 20 possible outputs, then any adversary can obtain the OPE key by studying the numerical bid of the eavesdropped cipher messages, despite the theoretical security.

Our breakthrough is a novel application of OPE termed rd OPE, which provides randomness in encryption outputs and is suitable for the problem of distributed fact production with a constrained input value range. The rd O PE build's technical difficulty is to keep the numerical ordering of encryptions from clear detectors that use clear OPEs. With the possible mapping between plaintexts and cipher texts predetermined by A, the cipher texts are theoretically determined prior to sensor deployment in such a way that the numerical ordering of cipher texts in clear detectors is possibly preserved. The following are two feasible problems for implementing rd OPE on sensor networks:

- The extra space required for each sensor to store the relevant rows of the RDOPE embark B.
- The fundamental notion of GD-VQ the main idea behind GD-VQ is that rd OPE, cryptographic hash, and the insertion of dummy readings, respectively, cement privacy, validity, and completeness.
- Particularly if the adversary is unable to discriminate between exact and dummy readings, intentional removal of ask results may result in the loss of dummy readings supposed to be provided in the task outcome.

5.1 PERFORMANCE ANALYSIS

- Asymmetric computational programs are often employed in encryption. In symmetric key cryptography, symbols are permuted or substituted, whereas numerals are modified in asymmetric encryption. Elliptic arc Cryptography concepts are applied in the field system. The elliptic arc arrangement is the standard IEEE approach in public-key cryptography. With its single key dimension, ECC provides comparable security to RSA.
-

6. CONCLUSION

In this research, we focus on the issue of verifiable top-k ask in two-tiered wireless sensor networks and propose ETQ-RIV, a convincing top-k ask processing framework with effect integrity verification. Each sensor node must comply with several encoded messages carrying the bid relationship as proof facts for verification, as well as their acquired sensing details, to make the ask outcome verifiable. The evaluation results show that ETQ-RIV may reduce the redundancy rate of the ask outcome and therefore lower both in-cell and ask communication costs, outperforming the accessible works in communication price.

REFERENCES

[1] Chia-Mu Yu, Guo-Kai Ni, Ing-Yi Chen, Erol Gelenbe & Sy-Yen Kuo, (2014) "Top-K Query Result Completeness Verification In Tiered Sensor Networks," Ieee Transactions On Information Forensics Security, Vol. 9, No. 1, Pp. 109-123.

[2] Yao-Tung Tsou, Chun-Shien Lu & Sy-Yen Kuo, (2013)"Motesec-Aware: A Practical Secure Mechanism For Wireless Sensor Networks", Ieee Transactions On Wireless Communications, Vol 12, No 6, Pp.2818-2822.

[3] Bagus Jati Santoso & Ge-Ming Chiu, (2014) "Close Dominance Graph: An Efficient Framework For Answering Continuous Top-K Dominating Queries", Ieee Transactions On Knowledge And Data Engineering, Vol 26, No 8, Pp.1854-1864.

[4] Lei Yu, Jianzhong Li, Siyao Cheng, Shuguang Xiong & Haiying Shen, (2014) "Secure Continuous Aggregation In Wireless Networks", Ieee Transactions On Parallel And Distributed Systems, Vol 25, No 3, Pp.763-773.

[5] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee & Chao Hsien Chu, (2013) "Enforcing Secure And Privacy-Preserving Information Brokering In Distributed Information Sharing",Ieee Transactions On Information Forensics And Security, Vol 8, No 6, Pp. 889-895.

[6] Rui Zhang, Jing Shi, Yanchao Zhang & Xiaoxia Huang, (2014) "Secure Top-K Query Processing In Unattended Tiered Sensor Networks",Ieee Communication And Information System, Huazhong University Of Science And Technology, Vol 25, No 3, Pp. 763-773.

[7] Daojing He, Sammy Chan & Shaohua Tang, (2014) "A Novel And Lightweight System To Secure Wireless Medical Sensor Networks",Ieee Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, Pp. 317-324.

[8] Mohamed M.E.A. Mahmoud, Sanaa Taha, Jelena Misic & Xuemin (Sherman) Shen, (2014) "Lightweight Privacy-Preserving And Secure Communication Protocol For Hybrid Ad Hoc Wireless Networks", Ieee Transactions On Parallel And Distributed Systems, Vol. 25, No. 8, Pp. 2078-2088.

[9] Emiliano De Cristofaro & Roberto Di Pietro, (2013) "Adversaries And Countermeasures In Privacy Enhanced Urban Sensing Systems", Ieee Systems Journal, Vol. 7, No. 2, Pp. 312-320.

[10] Omar Hasan, Lionel Brunie, Elisa Bertino & Ning Shang, (2013) "A Decentralized Privacy Preserving Reputation Protocol For The Malicious Adversarial Model", Ieee Transactions On Information Forensics And Security, Vol. 8, No. 6, Pp. 950-960.