IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
Research Paper Journal Volume 10, Iss 08, 2021

CHECKING AND GRADING THE COMPLETENESS OF TOP-K QUERY RESPONSES IN TIERED SENSOR NETWORKS

[#1]**Mrs.SHAGUFTHA BASHEER,** *Assistant Professor*

[#2]**Mr.PURAM SRINIVAS,** *Assistant Professor*

Department of Computer Science and Engineering,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT

A great number of applications for wireless sensors call for the collection of essential sensor data from the area in which they are deployed. Within the aforementioned applications, sensor nodes are responsible for the continuous transmission of data to storage nodes for a predetermined amount of time. Sending newly discovered data to the Top-K rule that makes the prediction is a crucial part of the process. The original content material details had some false information added to it so that attackers who had gained access to the sensor and storage nodes couldn't access the data they were after. In the event that an adversary is successful in penetrating the security of the storage node, there is a good chance that fake data will be sent to the command system. Steganography, when combined with the add-up complete signature method, shields data from vulnerabilities in the existing security system while also guaranteeing the message's validity. An indexing-based construct has been devised in order to guarantee that the database record's resources are available before the command delivers data to storage nodes.

Key Word: Vulnerabilities, Top-K rule, Guarantee that the database record's

1. INTRODUCTION

Since there may be prejudice between the authority (and owner of the contacts) and the entity that compiles the records, storing sensed data for archive and query response in sensor networks is important to ensure transparency. This is especially true when the parties may be biased. By configuring the connection strategy in this area, the regime can retrieve sensor readings through problem interrogation. Storage nodes, which have a lot of storage capacity, make up most of the basic level. Construction began with the level with the fewest resources and most traditional detectors. The relevant storage node receives readings. The storage node answers governing body questions and backs up typical sensor data. The request aims to achieve result integrity by speeding tag detection communication and encouraging a strong anonymization architecture that uses dummy scanning methodologies. Order-preserving encryption (OPE) is often used in catalog decryption. Unfortunately, literature usually assumes that one person wrote and encoded all texts. However, we will not debate this now. Given the potential sensor reading range constraints, which are usually mentioned and recorded in hardware specifications, the relationship between plaintext and encrypted text may become obvious in the future. Given these limits, these readings may be limited. Although theoretical security protections prevent it, a hacker can obtain the Order-Preserving Encryption (OPE) key by studying the numerical bids of intercepted cipher communications. This may happen if each detector can independently produce 20 findings.

Many sensor nodes have accurate top-k readings thanks to everyone's efforts. Comparing sensor data from different sensor nodes may show that the effect is only partially existent. Combination refers to adding additional data and ending verification. It balances communication labeling and partial search result naming. Distributed information sources that send sensed data to a proxy node were used to study the top k ask results' integrity. Even with insufficient readings,

detectors must provide cryptographic one-way hashes to the storage node for ask-execute completeness.

The Sensor Measurement Quality (SMQ) system employs sensor readings of established connections to create a verifiable entity from external factual information and sensor data. This verified entity uses sensor readings from established connections. It's impudent for Sensor Management Query (SMQ) to produce an aggregate tree structure with sensor nodes. Potential attackers can learn the likely range of sensor reading values by leveraging the SMQ bawdy index. This knowledge could be invaluable. In sensor network data collecting, the rule may indicate an unequal link. This requires a fundamental component that preserves felt data and encourages inquiry-based replies. This page describes the linked device and how the guiding concept transmits sensor reading requests.

All of the intermediate stratum was made of storage nodes, also called storage-rich nodes. In the base layer, modest sensors with limited capacities monitor the environment. Sensor nodes are usually divided into division groups in architectures with numerous overhead tiers.

encourage simulated reading-based anonymization framework development. This approach should simplify communication and make it harder to detect. OPE is often utilized in encrypted catalog reclamation. Unfortunately, the literature claims that a single controlling authority generated and encoded every detail, which contradicts our circumstance. The sensor array's potential allows plaintext-ciphertext correlations. Hardware requirements generate low-level measurements.

1. RELATED WORK

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

If a workable anonymization framework that's based on simulated reading is going to be developed, the complexity of intercommunication needs to be simplified first, even if that means there will be less opportunities for detection. In the context of encrypted catalog reclamation, OPE is a phrase that is used rather frequently. It is unfortunate that the literature makes the mistaken assumption that all of the information was developed and encoded by a single governing body. This assumption is wrong given the current state of affairs. The tremendous potential of the sensor array makes it possible to find correlations between plaintexts and ciphertexts. The measurements represent low-level numbers that are created from the requirements of the hardware.

Privacy and Integrity Preserving Range Queries in Wireless Sensor Networks

The approach for data anonymization that is based on order-preserving encryption (OPE) attempts to reduce the complexity of communication and the expenses associated with data detection while retaining data accuracy. On the other hand, the body of scholarly literature gives the impression that the generation of information and encryption may be under the control of a single government. When the connection between plaintext and encrypted data is made public, the security of a certain number of sensor readings is compromised. Two methods that can be utilized to assure the dependability and authenticity of data are the Markel hash tree and proximity manacles. Check to see if the findings of the research contain any informational items that provide a response to the inquiry or that attempt to answer it. In the context of sensor networks, I propose the application of bloom filters as a means of alleviating the financial burden brought on by intercommunication between sensor nodes and storage nodes.

SafeQ: Secure and Efficient Query Processing in Sensor Networks

On the other hand, storage nodes are separated from potential attackers by virtue of the significance they hold in the network. This article explains Safe, a mechanism that was developed to stop adversaries from accessing sensitive data by using sensor-collected data and sink-reissued

requests as a means of obtaining the information. Additionally, autonomous observers are able to monitor the status of resolved storage nodes thanks to Safe Q. The innovative data encoding and interrogation technology developed by Safe Q preserves users' privacy by enabling a storage node to carry out encoded questioning on encoded data without requiring the node to make any adjustments to the way it makes decisions in real time. Our intention is to make use of the data production mechanism known as neighborhood chains. This method enables a sink to confirm the accuracy of the result of a query while also protecting the integrity of the data by limiting the amount of information that is included in the output to only that which is significant.

Top-k Monitoring in Wireless Sensor Networks.

In order to make the most of various wireless sensor applications, superior observational approaches are required. This assumption is in line with the fact that a FILA, a low-power watching device that improves the semantics of the top k enquiries, is readily available. In order to prevent unnecessary sensor updates, it is essential to evaluate a sieve at each and every individual sensor node. Inadequate sieve sceneries and the addition of a request for reconsideration as part of the forward improvements are two significant issues that affect the accuracy and effectiveness of the FILA loom. We propose enhancing a query reevaluation system so that it can successfully examine a large number of sensor updates all at once. Utilizing ingenious optimization strategies allows for the tag to be sidestepped. A design with a skewed sieve placement was developed in order to successfully lower the amount of energy consumed and improve the bond's durability.

It is also anticipated that two unique sieve techniques, namely the furious and the languid approaches, will emphasize the finding of unambiguous instances of relevance. These strategies are referred to as the fast and slow approaches, respectively. In addition, we widen the talents of the algorithmic programmer to include a number of relevant inquiry possibilities. For example, we provide outputs that are arduous, imprecise, and engaging. The effectiveness of the FILA approach that has been suggested is investigated in great detail utilizing precise data traces. According to the findings, FILA performs better than TAG-based and range caching strategies when it comes to the durability of calls and the amount of power that they consume over a wide variety of call configurations.

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

Distributed draws are becoming more frequent as mobile devices with Internet connection and location awareness improve. This technology lets many users collect and share location-based data. A geolocation system with a data antenna and accurate information providers.

Customers and local business service providers (LBSPs) comprise the framework. Location-based service providers (LBSPs) obtain POI data from data collectors. These LBSPs allow users to request the top-k POIs in a region. The data collector collects POI ratings from reliable sources.

A characteristic with the highest k-score and strong relevance to the POI. Finally, unaddressed LBSPs can produce inaccurate search results for a variety of malicious motives, including poll manipulation for financial gain. Two unique methods for identifying fake top-k query results are presented in this dissertation to help users implement and use the selection process as intended. These dissertation strategies were created. Our technology is extensively studied and analyzed to ensure its efficacy and reliability.

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.

ISSN PRINT 2319 1775 Online 2320 7876
 Journal Volume 10, Iss 08, 2021

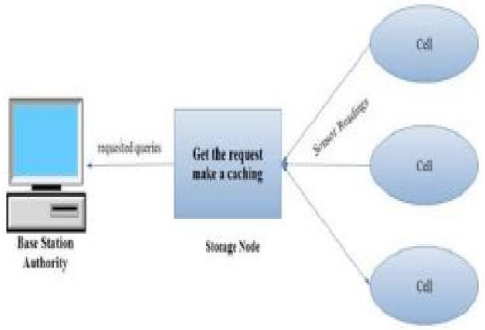
Additional evidence generates a message digest to confirm the specifics. The message will be read by the sender before being forwarded to the device. By comparingthe freshly generated digest with the corresponding retrieved message and cross-referencing them, the handset oversees confirming the message 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 . 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 . It is used to assess the validity and thoroughness of the investigation. The technology used by the verifiable asks processing method involves sending cryptographic one-way hashes.

Storage nodes, even when they do not have to fulfill 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 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

Sending data over many channels requires several secure protocols to prevent intruders from obtaining data. The standard method for protecting sensitive data includes verification and breach prevention. When more evidence supports the standards, a message digest is constructed. The sender will carefully review the message before sending it to the receiver. To validate the message digest, the handset compares the freshly produced digest to the recovered message. This insures digest correctness.

We prefer the opposite party adjust the communication platform material if they disagree. Cross-check delivers data to nearby sensor nodes for verification. The owner can verify the request by comparing sensor node data to neighbouring ones. A hybrid approach combines overarching strategies. Check if the query is complete. Requests are verified using one-way cryptographic hashes.

Two-tier sensor networks exchange data between sensor and storage nodes. Central nodes receive data from storage nodes. Storage nodes must do this regardless of data volume. Due to the data's relevance, a two-level design ensures authenticity and secrecy. After an attacker compromises information, the top-k ask method identifies

ISSN PRINT 2319 1775 Online 2320 7876
Research Paper **Journal Volume 10, Iss 08, 2021**

erroneous results from defeated nodes to the owner. Integrating many data links lets owners evaluate correctness.

The ask conversion component facilitates sensor node settlement detection. Information irrelevant to compromised nodes is leaked. Vanquish nodes and settlement detectors may cooperate, according to random testing. To ensure data accuracy, the owner randomly evaluates surrounding sensor nodes. The advanced load design RW determines sensor node resolution. The design is based on network node observations. Several methods allow the data owner to verify correctness and completeness.

Command issuing is essential for sensor data collection in tiered sensor networks. Top-k queries are basic querying algorithms due to their widespread use. Top k inquiries reduce unnecessary sensor readings. Rival canisters gain perceived data by intercepting sensor networks. Storage nodes controlled by the enemy can relay inaccurate data to the command center. How resolved storage nodes fragment the query result and offer an incorrect query result to deceive the authorities is critical. This is done by substituting answer portions with real readings.

VQ methods maintain stratified sensor networks' top-k ask effect without compromising dependability. Dummy readings and a novel anonymization architecture are used. Rope provides privacy using randomized and distributed bid-maintaining encryption. Although it simplifies theoretical and practical communication, AD-VQ-static may impair aptitude test accuracy. Due to their massive capacity, storage nodes can store plenty of data. Overdriven interactions allow these nodes to quickly and efficiently transfer data to multiple intermediary nodes. Without instructions, storage nodes can collect allies' cells.

Epochs coordinated node temporal coordinates. Two steps are needed to study information flow. During fact reporting, detectors validate and assign findings to the strongest storage node. Starting with each era, all sensors enter this time period. Party A's question is answered by the storage node in the second stage. This conclusion mentions HMAC hashing.

Say two people have exclusive private keys. A message associated to HMAC(m) assures that the data are authentic. Communication and discovery chances are assessed using integrity verification techniques.

ADVANTAGE:

To ensure that one's privacy is protected, a narrative surrogate reading-based anonymization skeleton is provided. The following step, which must be taken in the case of tiered sensor networks, is to validate the outcome of the top-k ask. The mission of the Privacy Foundation is to develop RODE, a randomized and decentralized encryption system that protects users' personal information. AD VQ-static is an excellent method for reducing the complexity of communication in both theoretical and practical settings, but this benefit comes at the expense of detecting capabilities. It was decided that the Keyed-Hash Message Authentication Code, or HMAC for short, would be the appropriate cryptographic primitive for the monetary system. Both sides are going to let the other one in on a little secret. The HMAC function and the message m that needs to be transmitted become coupled when the HMAC function is applied to the message m that needs to be transmitted. This link will take you to information about the application that is currently being evaluated.

EFFICIENCY AND SECURITY GAP

Nevertheless, despite the fact that previous research have been conducted, there are still issues that need to be resolved. The computational complexity of hybrid configuration communications is denoted by the notation O(n2). The Mote Sec-Aware design cannot work with large-scale networks because of this incompatibility. The usage of symmetric cryptography in KLM is made less effective due to the fact that the leader and sensor nodes in the network share an encryption key. Dominance Graph is designed to function properly in settings that are all the same. It is normal practice to

conduct numerous database searches in response to a client's request for comparable data in order to locate the data in question. If even one of the sensor nodes is breached by an adversary, they will soon have access to the symmetric key that all of the sensor nodes share. The verification method is used at each successive level of the process.

AUTHORITY DATA VALIDATION PROCESS

The government makes use of the essential steganographic decryption methods in order to recover any information that may have been concealed within a character. After the data has been retrieved, it is absolutely necessary to decode it via asymmetric key encryption. In order to maintain the confidentiality and authenticity of the data, it is necessary for both the government nodes and the sensor nodes to encrypt and decrypt the information. Asymmetric key encryption, which encrypts the message using the sender's public key, is utilized in order to ensure the confidentiality of the communication. The owner is the only person who can decode the content, which prevents unauthorized access.

The content may be decoded in the event that the private key is made available. Due to the inherently challenging nature of obtaining the decryption key, the adversary's ability to modify or extract the data will be effectively thwarted. The overhead method is used to ensure that a communication's confidentiality is maintained since only the person who is in possession of the correct decryption key may read a message that has been signed by the sender. The owner of the data will only share the decryption key with reliable people in the community.

Using message digesting and asymmetric key encryption, the second stage in confirming the authenticity of the facts is to make certain that the factual content that was sent by the sender has not been altered in any way. This method ensures that the facts are correct and comprehensive before they are sent through a communication medium. The regime is responsible for decrypting the data and keeping the database up to date with data from the sensors. The database will save any pertinent information regarding the sensor's environment that is gathered. Each unique sensor ID will be connected to its own individual entry in the database.

5. ALGORITHM/METHOD SPECIFICATION

The rdOPE Scheme Motivation:

OPE is now standard for decrypting and recovering encrypted data. Unfortunately, the essay implies that a single government agency created and encrypted all data. However, we won't discuss this today. It is important to remember that the hardware specs will limit sensor readings. The restricted number of interpretations may reveal the relationship between plaintexts and cipher messages without the recipient's knowledge. If the detectors have a limit on outputs, an adversary could find the OPE key by studying intercepted encrypted communications' numerical offers. Despite potential patches, this vulnerability remains.

Our research introduces rd OPE, a unique order-preserving encryption (OPE) method. This unique method solves fragmented fact creation in a limited input value range by randomizing encryption outputs. The biggest technical problem in creating the third O PE is maintaining the sequential ordering of encryptions to avoid being detected by clear detectors that use clear OPEs. Entity A chooses the plaintexts and ciphertexts for the sensors before deployment based on a relationship. This choice was intended to protect clear detectors' numerical ciphertext classification capacity. Using randomized differential privacy (rd OPE) in sensor networks provides two major challenges: - Data storage space needed by each sensor to track RDOPE embark B rows. The fundamental GD-VQ theory. GD-VQ protects data security, validity, and completeness using rd OPE, cryptographic hashes, and false readings. Due to the deliberate deletion of query results, the adversary may miss dummy readings in the task

conclusion if it cannot distinguish between actual and dummy readings.

PERFORMANCE ANALYSIS

The process of encryption frequently makes use of computing programs that are asymmetric. In asymmetric encryption, the integers cannot be altered in any way; whereas, in symmetric key cryptography, the symbols can be interchanged or permuted in any way. A portion of an ellipse that contains a curve is known as an elliptic arc. The field system uses cryptographic concepts to protect sensitive data. In the field of public-key cryptography, elliptic arc arrangements are a common type of configuration, as specified by the IEEE standard. ECC offers the same level of security that RSA does despite having its own distinctive key dimension.

6. CONCLUSION

The validated top-k inquiries in two-tiered wireless sensor networks are the primary topic of investigation in this research. Integrity verification is made possible by the ETQ-RIV framework, which is a top-k query processing system. To ensure that the outcome can be independently verified, it is necessary for each sensor node to comply with a variety of encoded signals. These proof facts may concern the bid relationship or the sensing data that the node has accumulated. According to the findings of the evaluation, ETQ-RIV has the potential to drastically cut down on the redundancy rate of the ask outcome, which ultimately results in reduced costs for in-cell and ask communication. This performance is superior to other ways that are currently being used in terms of the cost of communication.

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

ISSN PRINT 2319 1775 Online 2320 7876
Research Paper , **Journal Volume 10, Iss 08, 2021**

Reputation Protocol For The Malicious Adversarial Model, Ieee Transactions On Information Forensics And Security, Vol. 8, No. 6, Pp. 950-960.