SECURITY AND HONESTY APPLICABLE TOP-K QUERY PROCESSING FOR DUAL LEVEL SENSOR NETWORK

BALE KALYANI
M.Tech Student, Dept. of CSE, Vaagdevi College of Engineering, Warangal, T.S

Dr.M.SUKESH
Assistant Professor, Dept. of CSE, Vaagdevi College of Engineering, Warangal, T.S

Abstract

In the two-level Wireless Sensor Network, resource-limited sensor works as low-layer to censor node data, and the upper layer of resources to store data and processing questions with rich storage nodes Works as sink. Traditional wireless sensor networks (WSNs) include many small devices with restrained strength resources and one or more sinks to which the sensors ship their measurements. Sensor nodes are normally fixed and the everlasting trade in bodily topology usually comes from the disappearance of a node resulting from the depletion of its battery. Privacy and integrity is the main road block Two-level sensor network applications. Storage Middle-class works between Nodes, which are sensor and between Sink, can be understood and allows the invaders to learn seriously Save data and query results securely on secure projects Question processing is weak, because they show non-negligence Information, and therefore, the invaders can estimate the data Domain knowledge and date history using data The result of the question. In this paper, we first recommend the above question the processing scheme that protects the sensor data privacy and the integrity of the result of the question. In order to maintain privacy, we make an index Collect data item using random heash for each sensor Do top range in working and changing the filter of the bloom filter and tops to maintain integrity, we distribute the database Algorithm to distribute and attach every data item Distributed information with data. Attached information It ensures that the sink can confirm the integrity of the result of the question.

Keyword: *Privacy Preserving, top-k query processing, Traditional wireless sensor networks.*

I. INTRODUCTION:

Among others, sensor nodes differ from nodes in advert hoc community within the communication pattern: while advert hoc network nodes may additionally touch any other node within the network, sensors nodes ship records most effective to the sinks. The variety of the sensors' radio is in well-known pretty short, consequently multi-hop conversation is wanted among supply sensor nodes and the sinks. As a result, the volume of visitors within the network is centered within the neighborhood of the sinks. It follows that in case of energy-homogeneous nodes inside the community – nodes in the neighborhood of the static sinks are the first whose power useful resource receives depleted. This additionally manner that the life of the community relies upon on those vital nodes within the location of the sink. One solution to conquer this drawback is to apply cellular sinks as proposed via some researcher inside the last few years.Two-Tiered sensor networks had been widely followed for their scalability and strength efficiency. A big wide variety of sensors [1], geared up with confined storage and computing capability, are deployed in fields. Some garage nodes, prepared with massive storage and powerful commutatingcapability, are deployed amongst sensors for storing measurement facts from the neighboring sensors. A sink serves as a terminal device that sends queries to the storage nodes and retrieves the sensor records of interest. Due to the importance of -tiered sensor network architecture, numerous commercial garage nodes, together with StarGate and RISE have additionally been developed. The garage nodes provide two foremost advantages in comparison to an unstructured sensor network model. First, the storage nodes are chargeable for

the collection, storage and transmission of the sensory facts from the sensors to the sink. The sensors save a substantial quantity of energy via getting rid of sensor to sensor relay transmissions in the direction of the sink and extend the life of the community. Second, the garage nodes have extra computing strength and storage potential than the sensors. Therefore, the sink can problem complex queries, along with the variety or pinnacle-okay queries, to retrieve several data gadgets in a single question. This saves the sensor nodes' energy and community bandwidth required for answering the sink queries. However, due to their importance in community operations, the storage nodes are greater vulnerable to attack and compromise. Attackers cannot only thieve the touchy facts at the storage node, however additionally leverage the query processing functionality of the storage node to feed fake records to the sink [2].We deal with the problem of privacy and integrity maintaining top-okay queries in -tiered sensor networks to shield towards garage node compromise. Our intention is to design scheme to permit storage nodes to technique top-k queries efficiently withoutknowing the actual price of information stored in them and permit the sink to hit upon misbehavior of storage nodes. Top-ok question processing, i.e., finding the ok smallest or biggest information gadgets collected from a distinct sensed area, is an essential operation in sensor networks [3]. Such pinnacle-okay queries permit customers to get their maximum favored environmental records consisting of pollutants index, temperature, humidity and so forth. Our preference of the top-okay question hassle is prompted from the truth that it could be viewed as a generalized version of variety question, which lets in the sink to examine numerous values with an unmarried question.Previous works which might be in -tiered sensor networks and intently related to ours are privateers preserving top-k queries and privateers keeping variety queries. Broadly, these works fall into classes: bucketingschemes and order maintaining encryptionprimarily based schemes. Note that we classify SafeQ into order maintaining scheme because in SafeQ scheme, sensors sort their size statistics earlier than encryption and the encrypted records items are stored in an ordered way inside the storage nodes to facilitate the comfy queries.

II. LITERATURE WORK:

Our pointschemes can be found Cloud computing and database domains this can be done It is divided into three categories: bucket projects, order protection Projects, and public key projects. Hacigumus & L. Proposed First Bucket Distribution Scheme for Encryption Data Queries [4] Allows the server to know accurate data without knowing anything Values hover and l. The maximum bucket problem was investigated for distribution and two secure question plans, for one One dimensional figure and other for multi-dimensional Data Agarwal and L. The adoption of the Balting Scheme Ordered to maintain a scheme for ideas and offers Data privacy protection Boldyreva et al. recommended two order Protect of projects. However, these are the plans Section ID has been discussed as security weaknesses. I Le et al., Recommend the range of processing of privacy protection Scheme for outsource database items in Cloud Computing, which is IND-CKA proved safe under the security model. However, this scheme cannot interfere with the highest queries Authentication for the sensor network Bonus based on public

key script graphics-based schemes and water has suggested database privacy - planning protection Essential, subset and range questions to support. Oh ET al a range of query questions presented on the basis of identity Encryption Lovers [5]. However, the public key cryptography usually the two-level sensor is unstable in the network itscompulsion complexity (software implementation) and System configuration / maintenance costs (hardware process). An important amount has been suggested to work Integrity for query results in two tire sensor networks. All these tasks require a lot Also information and an extra validation procedure the result of the question. We show that the authenticity of our righteousness Mechanism is more expensive than they have.

The first venture of top-okay querying on the stored data is that the sensor statistics is in an encrypted layout on the storage node and for this reason, the garage node cannot execute a top-ok question without the ability to evaluate the statistics objects with every other. To deal with this assignment, we observe that a top-k query may be approximated by using the correct range question and the uniformly distribution of sensor facts enables this approximation. First, we describe an information distribution transformation method torework the arbitrary sensor records distribution into an approximate uniform distribution. Second, to keep privateers of sensor records, we describe a set of rules to construct an IND-CKA comfy privateers preserving index at the converted records the use of pseudo-random one-manner hash features and Bloom filters. Third, using prefix primarily based strategies, we transform lesser than and more than comparisons into equality checking, which most effective involves set membership verification operation at the Bloom filter indexes. Finally, we describe a variety estimation algorithm to convert a top-k question right into a unique variety question, referred to as top-range query, and enable the storage node to system the query on the comfortable Bloom filter indexes [6]. The second undertaking is to verify the integrity of the query effects. Towards this, we propose a singular data partition algorithm to partition the statistics gadgets into periods. We describe an embedding method to embed the interval information into the corresponding facts gadgets earlier than encrypting them. We gift an index choice approach to assure that the encrypted data objects are embedded with the perfect interval facts wanted for integrity verification by the sink node. The c programming language information permits the sink to stumble onwhether or not garage nodes have made any change to the query effects.

III. SYSTEM IMPLEMENTATION:

Our proposed scheme addresses the first art limit IND-CKA through a combination of security providers Range seriousness and data index generation techniques. The index stabilizes the invaders against the industrialization Reduce data values from question processing information.We undertake the system version utilized in existing privateers preserving querying processes [7] for two-tiered sensor networks. First, we assume that, all of the sensors and the garage nodes are loosely synchronized. Under this assumption, we divide the time into a series of constant duration time slots. In every time slot, a sensor collects more than one integer records objects, whose minimal and maximal possible values are known. At the

stop of a time slot, the sensor submits these statistics gadgets to its closest storage node. Second, every sensor stocks symmetric keys with the sink: a common key and a secret key. The commonplace secret's shared among all of the sensors and the sink. The secret key is shared between a given sensor and the sink. These two keys are saved in tamper-proof hardware and consequently, could not be compromised even supposing the sensors are captured by means of attackers. Third, the sensors may acquire multi-dimensional statistics. In thiscase, the sensors compute a score for every multi-dimensional statistics, and then permit the sink to question on these scores, andmethod adopted in preceding methods. Without lack of generality, we anticipate that top-k queries are accomplished on one-dimensional facts and the sink is interested inside the okay smallest information gadgets in the sensed information.

TOP –K QUERY:

Our approach to executing pinnacle-k queries at the sensor statistics is to transform the top-ok question into a top-variety question. The intuition at the back of this is that, directly acting top-k queries on a fixed of sensor records gadgets calls for comparisons among them. But, given the prefix club scheme from the previous section, we can test if a selected range of query prefixes are matched via any of the .

SYSTEM ARCHITECTURE:

stored prefixes inside the Bloom filter. This forms the premise of our approach wherein we transform the pinnacle-okay question into a suitably crafted variety query, to be able to gain the identical effects because the pinnacle-ok query. We next describe the info of this change [8].

BLOOM FILTER INDEX:

At this stage, we define a view to store the index Data item is not possible in such a manner that is not possible for storage Node to get any information related to the use of stored values The power or attack attacks described in the previous Note section, in time slot T, we assume that all sensors Share a slightly integrated secret key KT with sink.The experimental effects display that the Bloom filter operations also introduce false positives that lead to non pinnacle-okay information gadgets to be transmitted to sink [9]. Using different quantity of hash functions outcomes in unique false positive charges. As below shows that indicates the fake positive costs, towards the case where we used three hashes and the case where we used one hash, on Bloom filter out checking out. Using 3 hash capabilities, on an average, can reduce ninety one.7% fake tremendous fee while using one hash feature. When m/n = eight, the false advantageous rate due to Bloom filters can be controlled underneath 10%

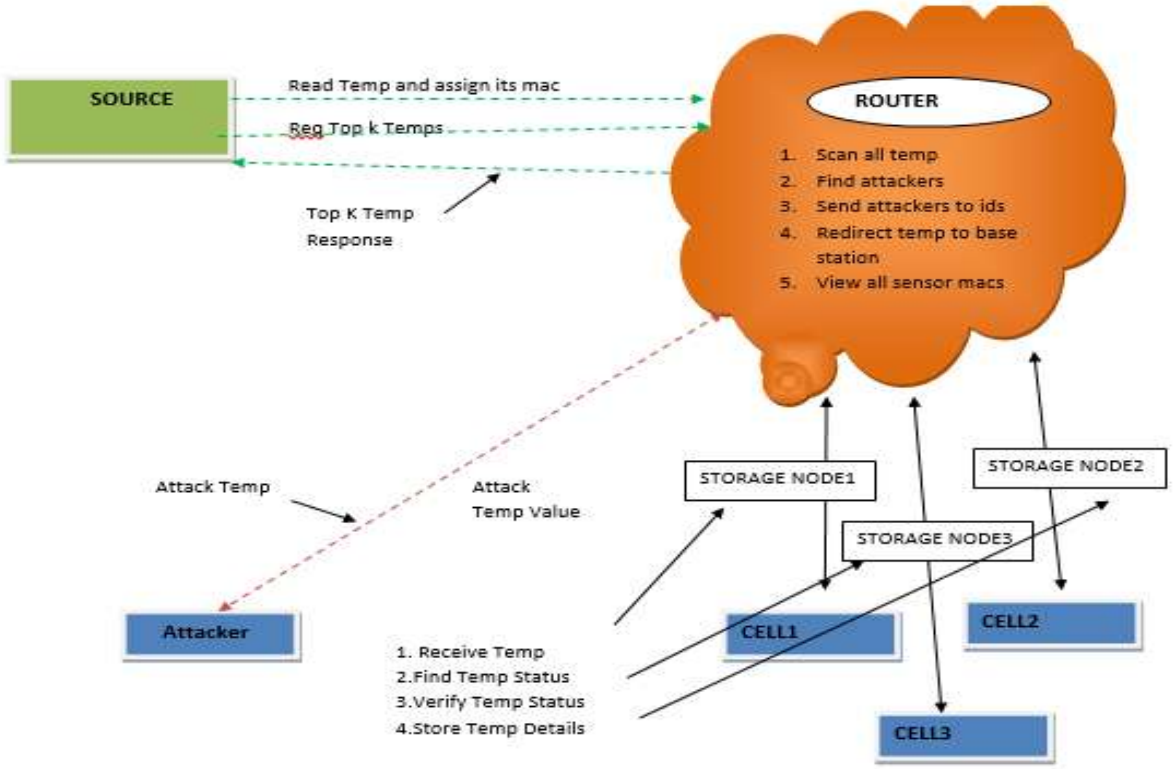

Fig.1 System Architecture

Fig.1 shows Architecture of Proposed implementation work. With several modules like source, and router and attacker with Cells.

ALGORITHM USED:

Top Range Computation:

Input: $[d'_0, d'_{n+1}]$, n, k, c
Output: $[d'_0, d']$

$low := d'_0$; $high := d'_{n+1}$;
while $low \leq high$ **do**
  $m = (low + high)/2$;
  $p = \frac{m - d'_0}{d'_{n+1} - d'_0}$;
  $f(d') = \sum_{j=0}^{k-1} \binom{n}{j} p^j (1-p)^{n-j}$;
  if $f(d') \leq c$ **then**
    $high := m - 1$;
  else
    $low := m + 1$;
$d' := low$;
return $[d'_0, d']$;

IV. CONCLUSION:

In this Approach, we propose the first cozy pinnacle-k question processing scheme that is cozy under the IND-CKA security model. The information privateness is assured by encryption as well as a cautious era of information indexes. We make key contributions in this paper. The first contribution is to convert a pinnacle-ok query to a pinnacle-range query and undertake membership trying out to check whether a facts item have to be covered inside the question result or now not. This transformation permits the storage node to locate ok smallest or largest information values without the usage of numerical contrast operations, which is a key method for the scheme to be cozy beneath the INDCKA safety version. The second contribution is the information partition, index choice, and c programming language information embedding technique. This approach guarantees that at the least one data item of each sensor gathered facts may be included in a query result and lets in the sink to verify the integrity of question end result without greater verification gadgets. Experiments display that the proposed scheme is bandwidth green and exceptionally practical. The techniques proposed on this paper can be doubtlessly beneficial for plenty different applications as properly.

V. REFERENCES:

[1] P. Desnoyers, D. Ganesan, H. Li, M. Li, and P. Shenoy, "Presto: A predictive storage architecture for sensor networks," in Proc. 10th HotOS, 2005, pp. 12–15.

[2] A. S. Silberstein, R. Braynard, C. Ellis, K. Munagala, and J. Yang, "A sampling-based approach to optimizing top-k queries in sensor networks," in Proc. 22nd ICDE, Apr. 2006, p. 68.

[3] I. F. Ilyas, G. Beskales, and M. A. Soliman, "A survey of top-k queries processing techniques in relational database system," ACM Comput. Surv., vol. 40, no. 4, pp. 11:1–11:58, Oct. 2008.

[4] H. Hacigumus, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proc. 21st ACM SIGMOD, Jun. 2002, pp. 216–227.

[5] E. Shi, J. Bethencourt, T.-H. Chan, D. Song, and A. Perrig, "Multidimensional range query over encrypted data," in Proc. 28th IEEE Symp. Secur. Privacy, May 2007, pp. 350–364.

[6] R. Zhang, J. Shi, and Y. Zhang, "Secure multidimensional range queries in sensor networks," in Proc. 10th ACM MobiHoc, May 2009, pp. 197–206.

[7] Z. Fu, F. Huang, X. Sun, A. Vasilakos, and C.-N. Yang, "Enabling semantic search based on conceptual graphs over encrypted outsourced data," IEEE Trans. Serv. Comput., to be published, doi: 10.1109/TSC.2016.2622697.

[8] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," IEICE Trans. Commun., vol. E98B, no. 1, pp. 190–200, Jan. 2015.

[9] Z. Zhou, Y. Wang, Q. M. J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 48–63, Jan. 2017.