Effective Privacy Preserving in Networks Using Merkle Hash Trees

A Sunitha[1], K Sudha reddy[2]

[1]working as an Associate Professor, Department of Computer Science & Engineering in Spoorthy Engineering College, Hyderabad, India

[2]pursuing M.Tech (CSE), Spoorthy Engineering College, Affiliated to JNTU-Hyderabad, India

Abstract:- The design of two-tiered sensing element networks, wherever storage nodes function Associate in performing intermediate tier between sensors and a sink for storing knowledge and process queries, has been wide adopted thanks to the advantages of power and storage saving for sensors yet because the potency of question process. However, the importance of storage nodes conjointly makes them enticing to attackers during this paper, we have a tendency to propose SafeQ, a protocol that forestalls attackers from gaining info from each sensing element collected knowledge and sink issued queries. SafeQ conjointly permits a sink to observe compromised storage nodes after they act. To preserve privacy, SafeQ uses a unique technique to cypher each knowledge and queries such a storage node will properly method encoded queries over encoded knowledge while not knowing their values. To preserve integrity, we have a tendency to propose 2 schemes—one victimization Merkle hash trees and another employing a new system referred to as neighborhood chains—to generate integrity verification info so a sink will use this info to verify whether or not the results of a question contains precisely the knowledge things that satisfy the query to boost performance, we have a tendency to propose Associate in Nursing optimization technique victimization Bloom filters to scale back the communication price between sensors and storage nodes.

Index Terms- SafeQ, Cypher, Merkle Hash trees, Range queries, optimization.

1. INTRODUCTION:

Wireless detector networks are wide deployed for numerous applications, like atmosphere sensing, building safety observance, earthquake prediction, etc. during this paper, we tend to take into account a two-tiered detector specification during which storage nodes gather information from near sensors and answer queries from the sink of the network. The storage nodes function associate degree intermediate tier between the sensors and also the sink for storing information and process queries. Storage nodes bring 3 main advantages to detector networks. First, sensors save power by causing all collected information to their nearest storage node rather than causing them to the sink through long routes. Second, sensors may be memory-limited as a result of information is in the main hold on on storage nodes. Third, question process becomes additional economical as a result of the sink solely communicates with storage nodes for queries. The inclusion of storage nodes in detector networks was initial introduced and has been wide adopted. However, the inclusion of storage nodes additionally brings important security challenges. As storage nodes store information received from sensors and function a very important role for respondent queries, they're additional liable to be compromised, particularly in an exceedingly hostile atmosphere. A compromised storage node imposes important threats to a detector network. First, the assaulter might get sensitive information that has been, or will be, hold on within the storage node. Second, the compromised storage node might come back cast information for a question. Third, this storage node might not embrace all information things that satisfy the question. Therefore, we wish to style a protocol that forestalls attackers from gaining info from each detector collected information and sink issued queries, which usually may be sculptures queue as vary queries, and permits the sink to find compromised storage nodes once they act. For privacy, compromising a storage node mustn't permit the assaulter to get the sensitive info that has been, and can be, hold on within the node, similarly because the queries that the storage node has received, and can receive. Note that we tend to treat the queries from the sink as confidential as a result of such queries might leak crucial info regarding question issuers' interests, which require to be protected particularly in military applications. For integrity, the sink must find whether or not a question result from storage node embraces cast information things or doesn't include all the info that satisfy the query. There are two key challenges in determination the privacy and conserving Privacy and Integrity in Wireless detector Networks integrity-preserving vary question drawback. First, a storage node must properly method encoded queries over encoded information while not knowing their actual values. Second, a sink must verify that the results of a question contains all the information things that satisfy the query and doesn't contain any cast data.

2. EXISTING:

In the existing system, the design of two-tiered device networks, wherever storage nodes function Associate in Nursing intermediate tier between sensors and a sink for storing knowledge and process queries, has been wide adopted attributable to the advantages of power and storage saving for sensors further because the potency of question process. However, the importance of storage nodes conjointly makes them engaging to attackers. So, the attackers simply will get sensitive data or they'll acquire cheap estimation on each sink issued queries and device collected knowledge

3. PROPOSED:

SafeQ protocol is planned that stops attackers from gaining data from each device collected knowledge and sink issued queries. SafeQ additionally permits a sink to discover compromised storage nodes after they move. We tend to propose SafeQ, a unique and economical protocol for handling vary queries in two-tiered device networks during a privacy- and integrity- protective fashion. To preserve Privacy, SafeQ uses a unique technique to inscribe each knowledge and queries such a storage node will properly method encoded queries over encoded knowledge while not knowing their actual values. To preserve integrity, we tend to propose two schemes—one victimization Merkle hash trees and another employing a new arrangement referred to as neighborhood chains—to generate integrity verification data such a sink will use this data to verify whether or not the results of a question contains precisely the knowledge things that satisfy the query associate optimization technique is additionally planned by victimization Bloom filters to considerably scale back the communication price between sensors and storage nodes.

4. METHODOLOGY:

4.1 SafeQ Environment Creation:

SafeQ may be a protocol that forestalls attackers from gaining data from each detector collected information and sink issued queries. SafeQ conjointly permits a sink to discover compromised storage nodes once they act. To preserve privacy, SafeQ uses a completely unique technique to inscribe each information and queries specified a storage node will properly method encoded queries over encoded information while not knowing their values.

4.2. Storage Node:

Storage nodes are powerful wireless devices that are equipped with way more storage capability and computing power than sensors. The storage node collects all information from the detector nodes. The storage node can’t read the particular price of detector node information. If the storage node making an attempt to look at the detector node information, sink observe mean of storage node.

4.3 Sink:

The sink is that the purpose of contact for users of the detector network. Whenever the sink receives a matter from a user, it 1st interprets the question into multiple queries and so disseminates the queries to the corresponding storage nodes, that method the queries supported their information and come back the question results to the sink. The sink unifies the question results from multiple storage nodes into the ultimate answer and sends it back to the user. Sink will sight compromised storage nodes once they misconduct.

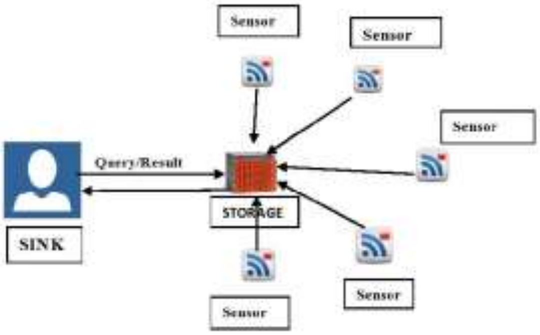

Fig. 1 Architecture of two tires sensor networks

4.4 Range Queries:

The queries from the sink are range queries. A range query “finding all the data items collected at time-slot in the range” is denoted as. Note that the queries in most sensor network applications can be easily modeled as range queries

4.5 Integrity Preserving:

The sink has to notice whether or not question result from a storage node embodies solid knowledge things or doesn't include all the info that satisfy the query. There are 2 key challenges in finding the privacy and integrity-preserving vary question downside. First, a storage node has to properly method encoded queries over encoded knowledge while not knowing their actual values. Second, a sink has to verify that the results of question contain all |the information things that satisfy the query and doesn't contain any solid data. To preserve integrity, SafeQ uses Two schemes. One is ‘Merkle Hash Tree’ and alternative is ‘Neighborhood Chains’. These 2 schemes give integrity verification data like Verification Object to visualize the integrity of a given question Result.

4.6 Privacy Preserving:

To preserve privacy, SafeQ uses a unique technique to code each information and queries specified a storage node will properly method encoded queries over encoded information while not knowing their actual values. Here sink, detector and storage nodes use a distinct magic functions like H,G,E for the detector collected information d1….dn and sink issued queries. detector conjointly applies secrete key Ki to the detector collected information and it sends to storage node at the side of id as Si to produce the privacy and conjointly to shield the sensitive info (ex. Military) from the attackers.

5. CONCLUSION:

We create 3 key contributions during this paper. First, we tend to propose SafeQ, a completely unique and economical protocol for handling vary queries in two-tiered detector networks in an exceedingly privacy- and integrity-preserving fashion. SafeQ uses the techniques of prefix membership verification, Merkle hash trees, and neighborhood chaining. In terms of security, SafeQ considerably strengthens the protection of two-tiered detector networks. in contrast to previous SafeQ prevents a compromised storage node from getting an affordable estimation on the particular values of detector collected information things and sink issued queries.In terms of potency, our results show that SafeQ considerably outperforms previous art for third-dimensional information in terms of each power consumption and cupboard space. Second, we tend to propose associate degree improvement technique exploitation Bloom filters to considerably cut back the communication price between sensors and storage nodes. Third, we tend to propose an answer to adapt SafeQ for event-driven detector network.

REFERENCES:

[1] P. Devanbu, M. Gertz, C. Martel, and S. G. Stubblebine, "Authentic data publication over the internet," J. Comput. Security, vol. 11, no. 3, pp. 291–314, 2003.

[2] H. Pang and K.-L. Tan, "Authenticating query results in edge computing," in Proc. ICDE, 2004, p. 560.

[3] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proc. ACM SIGMOD, 2005, pp. 407–418.

[4] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," in Proc. DASFAA, 2006, pp. 420–436.

[5] H.Chen, X.Man,W.Hsu, N. Li, and Q.Wang, "Access control friendly query verification for outsourced data publishing," in Proc. ESORICS, 2008, pp. 177–191.Preserving Privacy and Integrity in Wireless Sensor Networks 1

AUTHORS

A SUNITHA, is working as a Associate Professor in CSE department at Spoorthy Engineering College, Nadargul Village, Near Vanasthalipuram, Sagar Road, Saroornagar Mandal, Hyderabad.

K SUDHA REDDY, pursuing M.Tech(CSE) from Spoorthy Engineering College Nadargul Village, Near Vanasthalipuram, Sagar Road, Saroornagar Mandal, Hyderabad.