Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

PRIVACY- AND INTEGRITY-PRESERVING ENTIRE RANGE QUERIES IN SENSOR NETWORKS

Pradip Krishnadeo Patil,
AITP,Vita, Sangli, Maharashtra, India *pradippatil8432@gmail.com
Nilesh Ashokrao Thorat
AITP,Vita, Sangli, Maharashtra, India *nileshthorat2006@rediffmail.com

ABSTRACT
The architecture of two-tiered sensor networks, where storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. However, the importance of storage nodes also makes them attractive to attackers. This paper we proposed **Paillier Cryptosystem** that prevents attackers from gaining information from both sensor collected data and sink issued queries. **To preserve Privacy,** A paillier cryptosystem is a modular, public key encryption scheme, using this scheme both data and query message are encrypted such that storage node can correctly decrypt messages of an encrypted query over encrypted data without knowing their value in the message. **To preserve integrity**, we propose two schemes—one using Merkle hash trees and another using a new data structure called neighborhood chains—to generate integrity verification information so that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query.
KEYWORD —Integrity, privacy, range queries,paillier cryptosystem**,** sensor networks.

INTRODUCTION

WIRELESS sensor networks (WSNs) have been widely deployed for various applications, such as environment sensing, building safety monitoring, earthquake prediction, etc. Advances in wireless communication and electronics have enabled the development of low-cost, low- power, multifunctional sensor nodes. These tiny sensor nodes, consisting of sensing, data processing, and communication components, make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks. WSNs can greatly simplify system design and operation, as the environment being monitored does not require the communication or energy infrastructure associated with wired networks [1]. WSNs are expected to be solutions for many applications, such as detecting and tracking the passage of troops and tanks on a battlefield, monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. Many sensor networks have mission-critical tasks and thus require that security be considered [2, 3]. Improper use of information or using forged information may cause unwanted information leakage and provide inaccurate results

The architecture of two-tiered wireless sensor networks as shown in fig(1), it consists of a storage nodes serve as an intermediate tier between sensors and a sink for storing data and processing queries, has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of the query processing. Storage nodes bring three main benefits to sensor networks. First, sensors save power by sending all collected data to their closest storage node instead of sending them to the sink through long Routes. Second, the sensors can be memory-limited because the data are mainly stored on storage nodes. Third, query processing becomes more efficient because the sink only communicates with storage nodes for queries. The storage node faces serious security challenge in hostile environment first, when the storage node is compromised the sensing data from the sensor nodes, the history of query requests and the corresponding query results are exposed. Second, it may cause heavy loss when the compromised sensor nodes return fake, forged or incomplete data for a query especially in military and commercial application. Therefore, developing a privacy- preserving and result-verification mechanism is of paramount importance, such that the authenticity and completeness of the query results can be verified as well as the privacy of the sensitive data is protected.

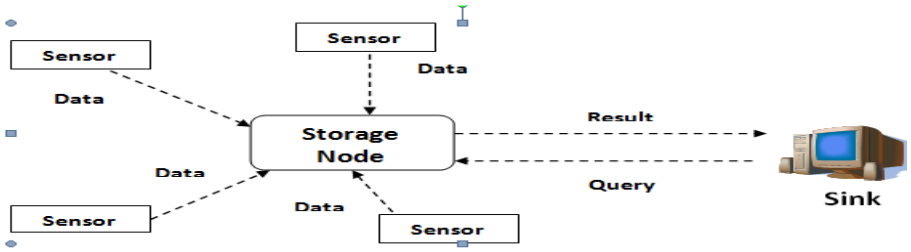


Fig (1). Two-tiered architecture of WSN.

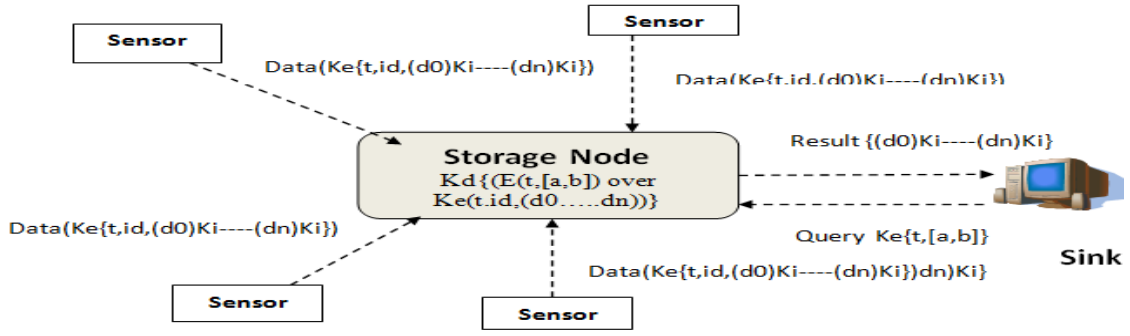
LITERATURE REVIEW

A Privacy- and integrity-preserving range query in WSNs has been studied in the recently [4], [5]. Sheng and Li proposed a scheme to preserve the privacy and integrity of range queries in sensor networks [4]. Proposes SafeQ [6], a protocol that prevents attackers from gaining information from both sensor collected data and sink issued queries. SafeQ also allows a sink to detect compromised storage nodes when they misbehave. 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 encoded data without knowing their value. To preserve integrity, we propose a Merkle hash tree [9] and new data structure called neighborhood chains that allow a sink to verify whether the result of a query contains exactly the data items that satisfy the query. In addition, it proposes a solution to adapt SafeQ for event-driven sensor networks.

Sheng and Li scheme uses the bucket-partitioning idea proposed by Hacigumus et al [8] for database privacy. The basic idea is to divide the domain of data values into multiple buckets, the size of which is computed based on the distribution of data values and the location of the sensors. In each time-slot, a sensor collects data items from the environment, places them into buckets, encrypts them together in each bucket, and then sends each encrypted bucket along with its bucket ID to a nearby storage node. For each bucket that has no data items, the sensor sends an encoding number, which can be used by the sink to verify that the bucket is empty, to a nearby storage node. When the sink wants to perform a range query, it finds the smallest set of bucket IDs that contains the range in the query, and then sends the set as the query to storage node. Upon receiving the bucket IDs, the storage node returns the corresponding encrypted data in all those buckets. The sink can then decrypt the encrypted buckets and verify the integrity using encoding numbers.

Proposed model

The proposed work uses two techniques for privacy and integrity preserving entire range queries in sensor network. During privacy preserving sensor send data in the form of 3-tuple {id, t, (d0,……, dn)} and sink also send data in the form of 2-tuple {t, [a.b]} to storage node, all this data items are encrypted using paillier cryptosystem. During integrity preserving wecan use a Merkle hash tree and neighborhood chain for verifying information given by storage node to sink. The proposed diagram of two-tiered architecture of wireless sensor network as shown in Fig 2



Where Keis the encryption key Kd is the Decryption key
Ki is the private Key

Fig: 2 Two Tiered Architecture of WSN.

PRIVACY FOR DATA

Paillier cryptosystem for privacy preserving of query and data. A paillier cryptosystem is a modular, public key encryption scheme, using this scheme both data and query message are encrypted such that storage node can correctly decrypt messages of an encrypted query over encrypted data without knowing their value in the messageas shown below fig 3.

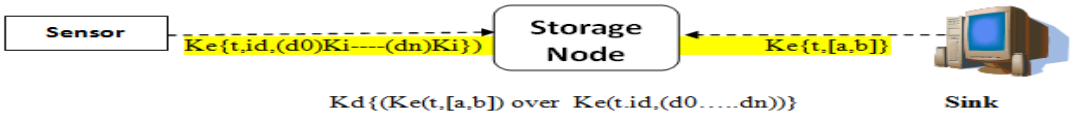


Fig 3.Idea of paillier Cryptosystem for privacy preserving.

Encryption and Decryption process of Paillier cryptosystem.

First, we generate public and private key for encryption and decryption.

Key Generation:-

1. The Public (encryption) key is (n, g)

Where n=p. q (p & q are two large prime numbers).

g is random integer belong to $\mathbb{Z}_n^2$.

$\mathbb{Z}n$ is a set of prime number.

2. The private (decryption) key is (λ, mu).

Where λ= lcm (p-1,q-1) = (p-1)*(q-1) / gcd(p-1,q-1)

mu= k^{-1} mod n

Where=k=L ($g^{\lambda(n)}$ mod n^2), where L (u) = (u-1) /n

Encryption process:-

1. Let m be a message to be encrypted with $m \in \mathbb{Z}n$.
2. Select random, nonzero r where $r \in \mathbb{Z}n^*$.
3. Compute the Ciphertext: - g^m. r^n mod n^2

Decryption process:

1. Ciphertext $C \in \mathbb{Z}n^{2*}$.
2. Compute Message $m \equiv L(c^{\lambda(n)} \bmod n^2) \cdot mu \bmod n$.

INTEGRITY FOR DATA

Merkle hash tree and a neighborhood chain scheme for integrity preserving of data. Using this scheme to generate integrity verification information, So that a sink can use this information to verify whether the result of a query contains exactly the data items that satisfy the query.To allow the sink to verify the integrity of a query result, the query response from a storage node to the sink consists of two parts: 1) the query result QR, which includes all the encrypted data items that satisfy the query; 2) the verification object VO, which includes information for the sink to verify the integrity of QR.

MERKLE HASH TREE:-

In the Merkle hash scheme, each time sensor wants tosend encrypted data items to a storage node, it first computes a Merkle hash tree, which is a complete binary tree over the encrypted data items, and then sends the only root value along with the encrypted data items to a storage node. The storage node receives a query from the sink, it first finds the data items that are in the range and computes the Merkle hash tree (except the root) from the data items. It sends the query result and the verification object to the sink. After receiving query result and verification object, it checks data items in the query result do satisfy the query, left and right neighbor of the Merkle hash tree and compute the root value is same as the root value in verification object. The Merkle hash tree used in our solution has two special properties that allow the sink to verify query result integrity. First, the value of the root is computed using aThe keyed HMAC function where the key is shared between the sensor and the sink .Using a keyed HMAC function gives us the property that only sensor and the sink can compute the root value. Second, the terminal nodes are arranged in an ascending order based on the value of each data item. Example of Merkle hash tree as shown in fig 4.

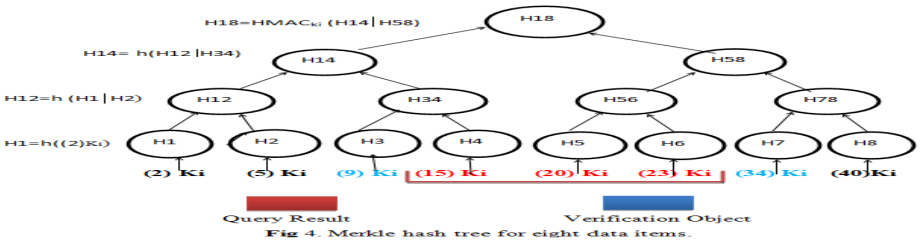


Fig 4. Merkle hash tree for eight data items.

Where Function 'h' is a one-way hash function such as MD5 or SHA-1

NEIGHBORHOOD CHAIN:-

In the neighborhood chain scheme sensor sends encrypted data item to the storage node. The storage node receives a query from the sink, it first finds the data items that are in the range. It sends the query result and the verification object to the sink. After receiving query result and verification object at the sink, it checks data items in the query result do satisfy the query and The corresponding verification object only consists of the right neighbor of the largest data item in the query result. Example of neighborhood chain as shown in fig 5.

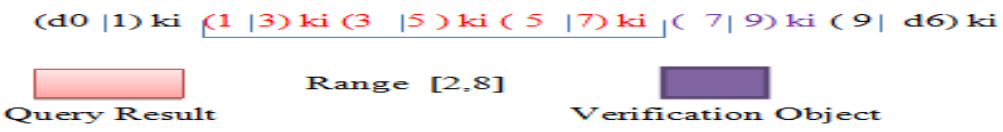


Fig 5. Example of Neighborhood chain

CONCLUSION

In this paper we propose paillier Cryptosystem for handling entire range queries in two-tiered sensor networks in a privacy- and integrity-preserving fashion. Paillier Cryptosystem uses the techniques of public key encryption scheme, Merkle hash trees, and neighborhood chaining. In terms of security, paillier Cryptosystem significantly strengthens the security of two-tiered sensor networks. Paillier Cryptosystem prevents a compromised storage node from obtaining a reasonable estimation on the actual values of sensor collected data items and sink issued queries

REFERENCES

[1] D. Estrin, et al., "Instrumenting the World with Wireless Sensor Networks," Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.
[2] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Comp. Mag., Oct. 2003, pp. 103–05.
[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.
[4] Sheng B, Li Q. Verifiable privacy-preserving range query in two tiered sensor networks. In INFOCOM'08, pp. 46-50. IEEE 2008
[5] ShiJ,ZhangR, ZhangY. Secure range queries in tiered sensor networks. In INFOCOM'09. Pp. 197-206. IEEE, 2009
[6] Fei Chen and Alex X. Liu "Privacy- and Integrity-Preserving Range Queries In Sensor Networks" IEEE/ACM, TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, DECEMBER 2012
[7] Rui Z, Jing S, Yunzhong L, et al. Verifiable fine-grained top-k queries in tiered sensor networks. In INFOCOM'10. IEEE, 2010
[8] H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proc. ACM SIGMOD, 2002, pp. 216–227.
[9] R. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE S&P, 1980
[10] J. Cheng, H. Yang, S. H. Wong, and S. Lu, "Design and implementation of cross-Domain cooperative firewall," in Proc. IEEE ICNP, 2007.
[11] Fei C, Alex L. SafeQ: Secure and Efficient query processing in sensor networks. In NFOCOM'10. IEEE, 2010