Privacy And Integrity Preserving Top-*k* *Query* Processing For Two-tiered Sensor Networks

ABSTRACT

- Privacy and integrity have been the main road block to the applications of two-tiered sensor networks
- The storage nodes, which act as a middle tier between the sensors and the sink, could be compromised and allow attackers to learn sensitive data and manipulate query results
- Prior schemes are weak they reveal the information,so the attackers easily collects the infomation
- we propose the first top-*k query* processing scheme that protects the privacy of sensor data and the integrity of query results
- To preserve integrity, we propose a data partition algorithm
- We formally prove that our scheme is secure under IND-CKA security model

EXISTING SYSTEM

- The storage nodes, which act as a middle tier between the sensors and the sink, could be compromised and allow attackers to learn sensitive data and manipulate query results
- Prior schemes on secure query processing are weak,they reveal information

DISADVANTAGES

- Reveals the infomation using Prior schemes
- Attackers collects the data

PROPOSED SYSTEM

- We propose the first top-*k query* processing scheme that protects the privacy of sensor data and the integrity of query results
- To preserve integrity, we propose a data partition algorithm
- we prove that our scheme is secure under IND-CKA security mode

ADVANTAGES

- It protects the privacy of sensor data and the integrity of query results
- To preserve integrity, we propose a data partition algorithm

System Requirements

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net
- Tool : Visual Studio 2010
- Database : SQL SERVER 2008

Conclusion

- In this paper, we propose the first secure top-*k query* processing scheme that is secure under the IND-CKA security model. The data privacy is guaranteed by encryption as well as a careful generation of data indexes. We make two key contributions in this paper. The first contribution is to transform a top-*k query to a top-range query and adopt* membership testing to test whether a data item should be included in the query result or not. This transformation allows the storage node to find *k smallest or biggest data values* without using numerical comparison operations, which is a key technique for the scheme to be secure under the INDCKA security model. The second contribution is the data partition, index selection, and interval information embedding technique.