Secure Range Search over Encrypted Uncertain IoT Outsourced Data

ABSTRACT

- Internet of Things (IoT) is an increasingly popular technological trend. The operation of IoT needs a strong datahandling capacity,where most of the data is sensor data. Limitations associated with measurement, delays in data updating, and/or the need to preserve the privacy of data can result in the sensor data being uncertain. Thus, one key challenge is "How do we ensure the privacy of data collected from IoT devices, particularly uncertain data, that are being outsourced to the cloud for analysis, storage and archival?". Searchable encryption (SE) scheme is a promising technique that allows the searching over encrypted (uncertain) data stored offshore. In this paper, we propose a secure range search for encrypted data from IoT devices. Specifically, we use homomorphic and order-preserving encryption (OPE) to encrypt data published by the data owners. We then use the k-dimensional tree (KD-tree) to build the data index. Our scheme is designed to ensure the privacy of the dataset, without affecting the efficiency of keyword search on the (encrypted) dataset.

EXISTING SYSTEM

- Internet of Things (IoT) is an increasingly popular technological trend. The operation of IoT needs a strong datahandling capacity, where most of the data is sensor data. Limitations associated with measurement, delays in data updating, and/or the need to preserve the privacy of data can result in the sensor data being uncertain. Thus, one key challenge is “How do we ensure the privacy of data collected from IoT devices, particularly uncertain data, that are being outsourced to the cloud for analysis, storage and archival”.

PROPOSED SYSTEM

- In this paper, we propose a secure range search for encrypted data from IoTdevices. Specifically, we use homomorphic and order-preserving encryption (OPE) to encrypt data published by the data owners. We then use the k-dimensional tree (KD-tree) to build the data index. Our scheme is designed to ensure the privacy of the dataset, without affecting the efficiency of keyword search on the (encrypted) dataset. We also demonstrate that our scheme can preserve both data and query privacy, as well as evaluating its performance to demonstrate efficiency.

CONTINUE

- In this paper, we apply OPE and homomorphic encryption simultaneously to encrypt the sensor data. Data owners obtain uncertain data from the IoT devices. They then use the KD-tree to organize the data. To ensure data privacy, they will use the OPE and homomorphic encryptions to encrypt the KD-tree and the dataset. Such data can then be outsourced to the cloud. When users wish to perform a range search, they should encrypt the query and then send that query to the cloud. When the cloud receives the query, it will conduct a search over the KD-tree and return the encrypted results to the users.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

CONCLUSION

- The diversity and range of IoT devices will grow as they are deployed in a broader range of applications, ranging from civilian (e.g. smart cities and emergency response) to military and battlefield (e.g. Internet of Military Things and Internet of Battlefield Things) and so on. This reinforces the need to efficiently manage uncertain and increasing amount of data from the IoT devices. To ensure the security of uncertain IoT data, particularly those outsourced to the cloud or the edge, we developed an effective indexing technique to support range searches on multidimensional encrypted data. Specifically, in the proposed scheme, we used the KD-tree to organize the objects to improve the retrieval efficiency.

REFERENCE

[1] H. P. Kriegel, P. Kunath, M. Pfeifle, and M. Renz, "Probabilistic similarity join on uncertain data," in *International Conference on Database Systems for Advanced Applications*, 2006, pp. 295-309. M. Roopaei, P. Rad, and K. K. R. Choo, "Cloud of Things in Smart.

[2] Agriculture: Intelligent Irrigation Monitoring by Thermal Imaging,“ *IEEE Cloud Computing*, vol. 4, pp. 10-15, 2017.

[3] S. Singh, C. Mayfield, S. Prabhakar, R. Shah, and S. Hambrusch, "Indexing Uncertain Categorical Data," in *IEEE International Conference on Data Engineering*, 2007, pp. 616-625.

CONTINUE

[4] Y. Tao, X. Xiao, and R. Cheng, "Range search on multidimensionaluncertain data," *Acm Transactions on Database Systems,* vol. 32, p. 15, 2007.

[5] D. X. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in *IEEE Symposium on Security and Privacy*, 2000, p. 44.

[6] B. Dan, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, *Public Key Encryption with Keyword Search*: Springer Berlin Heidelberg, 2004.