TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 2047 - 2049

Performing Secured Range Search on Uncertain Data Outsourced in IoT

[1]P. Gnanendra Prasad, [2]Uma Priyadarsini

[1]UG Scholar, [2]Assistant Professor (SG),
Department of Computer Science and Engineering,
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai
[1]gnanz06@gmail.com, [2]umapriyadarsini@saveetha.com

Article Info
Volume 82
Page Number: 2047 - 2049
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *12 January 2020*

Abstract
Nowadays various technologies are being invented in our day to day life for various purposes. These technologies are being used for their respective advantages. One among those technologies is the Internet of Things (IOT). IOT is playing a major role in the current generation. Huge amount of data in being stored and produced, in and from various IOT devices. One has to ensure that those data are being safe from the various external factors. Though the data are being encrypted, some of the data are being tampered by various other methods. In IOT, most of the data are sensor data which leads to uncertainty.

Keywords: *range search, searchable encryption, probabilistic density function, sensors*

1. Introduction

Though many technologies are being invented in the current world, IOT is playing a major role in many people's lives for various purposes. The IOT devices process the data in various ways based on the purposes. In many IOT devices, the data are outsourced by encrypting it for secured transmission. Those data can be highly confidential and private, where the user wishes not to be accessed by any other unauthorised or illegitimate parties. In IOT, hardware equipment like sensors, actuators are often used. The sensor collects the data from the surroundings and outsources it to the destined location or device. Those data are often stored in various databases, but before reaching the database the data might be uncertain and not secured which is a vulnerability for the users and their data. The attacker might use this opportunity to access and tamper that data for the purpose he wishes to do. So, the ways to process those uncertain data in an efficient manner is considered as a major aspect to be solved immediately.

The basic query used for the uncertain data in IOT devices is Range Search, where the primary function is to obtain data inside the given range boundary. The range search is often used in various real world applications, and one among them is the IOT devices in agriculture lands for keeping a record of the surroundings, level of humidity and other contamination factors present in the surroundings. The role of the sensors is to collect three different data values, and is considered as a 3D object. Sometimes, due to technical glitches like noises and failure in the equipment, the data being received might be uncertain, in that case each object is denoted by a particular uncertain region and a function called Probabilistic Density Function is implemented. Generally, our farmers might face difficulties in obtaining the precise data manually. So, the range search technique gives a hand to us in this scenario. Using it, we can analyse and also predict the range that doesn't have normal conditions. This helps us to notice the importance of range search in our daily applications.

Searchable Encryption techniques can often be implemented for searching any encrypted data. Even after using enhanced schemes for these applications, some factors like uncertain data, and improper prediction of the nature by the IOT sensors, often leads to complications in the process of efficient search on those encrypted data. In this paper, the challenging scenario to design a secure range search for supporting the given respective queries of uncertain outsourced data in IOT devices has been considered as a primary topic to be focused on.

November-December 2019
ISSN: 0193-4120Page No. 564- 568

2. Literature Survey

In order to perform a literature survey based on the topic chosen, various research papers have been collected and analysed for gathering some information regarding the project and its implementation. It has been noticed that, the authors have used U-Quad tree for arranging the uncertain data to support the range search technique. A cost model for building an efficient Quad tree has been developed, if the data collected in the dataset is uneven, it would make the tree to be unbalanced. Which in-turn leads to overhead of time and incurs significant storage of the data. The management of uncertain data has obtained a traction among various researchers, mainly due to its applications in the different kinds of domains. It is an efficient way for conducting data analysis, with the help of enabling a quick search of most relevant data. In the recent years, lots of range search schemes on uncertain data has been shown in the literature, where most of them use some random indexing techniques for increasing the retrieval performance. Some of the often used retrieval structures are R-tree, U-tree, Quadtree, etc. In those 4 structures, a strategy known as "Equality Strategy", where equal size of resources are allocated to each uncertain data. But as a result, it can't address various uncertain region sizes at the time of index construction. In order to solve such problems in other research papers, they have used Quad tree for organizing the uncertain data that is being stored. The Quad tree is a tree structure that partitions space for the data where a d-dimensional number of space is recursively further subdivided into 2^d number of regions. In each step of the partitioning process the provided space will be further divided into 2^d equal number of parts. However, implementing this method consumes lots of space and time. Like we discussed before, the existing system just supports range search on uncertain data in plaintext.

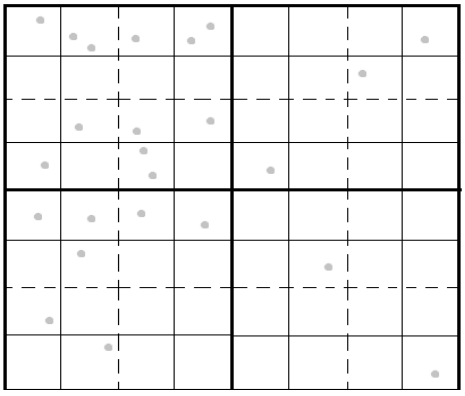

Figure 1: Example structure of a Quad tree

3. Existing System

We can notice that the Searchable Encryption helps the data owners in searching the encrypted data, which might also be in cloud. The present SE techniques can be separated based on the encryption methods, like public key cryptography method and symmetric key cryptography method. In the paper proposed by Song et al, we can notice that various operations have been performed in the cipher text domain. Similarly, a homomorphic encryption method was implemented by Paillier et al in the same research for additional support to it. The current research on range searches over many dimensional uncertain data having an arbitrary PDF value, which primarily follows the paradigms like filtering and verification of those uncertain data. By increasing the level of effectiveness of the index structure, few objects might be filtered at a threshold value without even calculating the probability of their appearances detail. The main drawback of the existing system is that they perform the searching technique only on the plain text but not encrypted data. And they also do not consider the features like sharing and data interaction.

The most vital medium for sharing and data interaction in the domain of IOT is the cloud, because of the benefits like low cost, high level of capacity and overhead reduction. Let's consider an example, the data owners can be benefit the first symmetric SE method, but eventually various other searchable encryption methods were proposed later. Such early kinds of works only provides support to the keyword search methods, where they are too simple when it comes to factors like functionality. Due to the rise in the enhancement of technologies, the complexity of the data is also being increased simultaneously. Anyhow, the earlier searchable encryption techniques are not sufficient enough for performing searches over the uncertain data.

4. Proposed System

In order to overcome all the previously enlisted problems, we are implementing a different technique for the range search of uncertain data, which is KD-tree. Its structure is binary space partitioned for organising the uncertain data collected from the sensors. KD-tree is primarily used for multidimensional space data retrieval. An efficient level of retrieval can be obtained by solving the flaws in the other indexing structural methods. Due to the reason that data from the IOT devices are often uncertain, so the range search for the encrypted data should also support the basic operations in order to complete the process successfully. There are 4 different modules in this project, data server, cloud server 1, cloud server 2, and the user. The sample model has been shown in the Fig. (2). it can noticed that the sensor object has a sensor ID, a collection of instances and its probability. The instances contains a d-dimensional with its respective coordinates. The data owner should be having various data sets which has to be outsourced to the cloud server. For enabling the capability to search over the encrypted data, the owner should first build an encrypted KD-tree by using those data sets he gathered at the beginning. Later, the encrypted data and the KD-tree data will be outsourced to the cloud server 1. If the user wishes to perform a range search, the user should encrypt the query and finally send it to the cloud server 1. When the data owner outsources

the encrypted KD-tree, the user must use a secret key of OPE for encrypting the respective query and later, sends the search token that is encrypted. At last, the cloud server 1 and server 2 will function mutually to search and find the encrypted KD-tree and thus it returns the results to the user respectively.

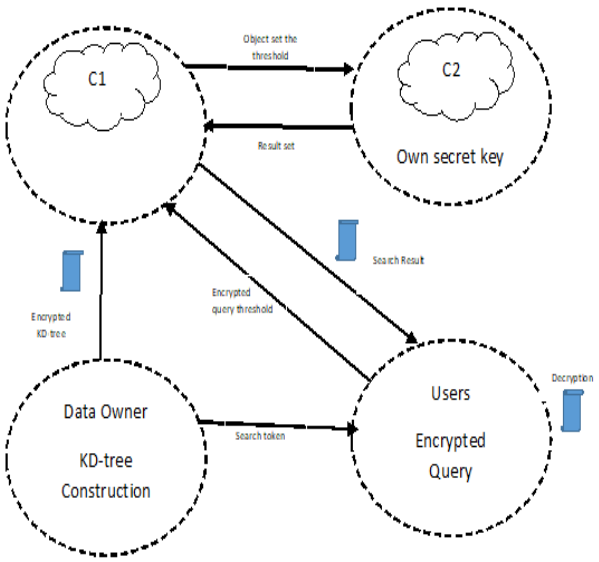

Figure 2: Model of the Proposed System

5. Conclusion

The usage and kinds of IOT devices will be gradually growing due to the different kinds of applications, from the basic needs of a human's life to the most advanced level like military, warfare, etc. so one cannot deny the usage of IOT devices in his/her daily life. Due to the various dependencies on IOT devices, we are forced to manage the uncertain and huge amount of data from those devices.

In order to provide security and privacy for the daily users of IOT device, especially for those where the data is outsourced to the cloud or edge, we have introduced an effective technique of data indexing which supports range searches on encrypted data. We have implemented KD-tree for organising the objects, so that the retrieval efficiency increases. And also, for supporting the operations over cipher text, we have also used OPE and homomorphic encryption technique.

Further researches are going to be conducted for introducing a prototype of the proposed scheme in our real world, which helps us to use the methodology for various other applications in our day to day life.

6. Result

Thus, by gathering various articles and references related to the project title, an intensive literature survey has been performed. It has been noticed that various authors have implemented different kind of techniques to perform a secured range search, by considering those parameters and instructions, a similar range search will be implemented over the encrypted data that is being outsourced in various IOT devices.

References

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

[2] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K.-K. R. Choo, "Fine-grained database field search using attribute-based encryption for e-Healthcare clouds," *Journal of Medical Systems*, vol. 40, p. 235, 2016.

[3] M. Roopaei, P. Rad, and K. K. R. Choo, "Cloud of Things in Smart Agriculture: Intelligent Irrigation Monitoring by Thermal Imaging," *IEEE Cloud Computing*, vol. 4, pp. 10-15, 2017.

[4] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A Practical Privacy-Preserving Data Aggregation (3PDA) Scheme for Smart Grid," *IEEE Transactions on Industrial Informatics*, 2018.

[5] Lakshmanan, V. S. Laks, Leone, Nicola, Ross, Robert, *et al.*, "ProbView: a flexible probabilistic database system," *Acm Transactions on Database Systems*, vol. 22, pp. 419-469, 1997.

[6] 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.