Protection of Location Privacy using Implement Mechanism for Large Data in IOT.

[1]Hardik S. Aghera, [2]Ashutosh A. Abhangi, [3]BirjuTank

[1]ME Scholar of Computer Engineering Department, Noble Group of Institutions, Junagadh, Gujarat, India

[2]Assistant Professor, Computer Engineering Department, Noble Group of Institutions, Junagadh, Gujarat, India

Abstract: Location privacy protection in existing methods is mostly using the traditional Anonymization, fuzzy and cryptography technology. Here propose location privacy Protection in use differential privacy constraint to protect location data privacy and utility maximization of data and algorithm in Internet of Things. In this case high value and low density of location data and here combine the utility with the privacy and build a multiple location information tree model. The index mechanism of differential privacy strategy is used to select data to the tree node accessing frequency. And Laplace implementation mechanism is used to add noises to accessing frequency of the selecting data. Here discuss and improve to explore the more efficient data structure to express location information in the process of location data Expression and propose more utility target functions.

***Index Terms*–Differential privacy, location privacy protection, location privacy tree, Internet of Things.**

I. INTRODUCTION

1.1 INTRODUCTION OF IOT.

Internet of Things (IoT) is represented as a global network which smartly connects different devices, system or human with self-configuring capabilities based on standard and interoperable protocols. The idea is to connect various devices or objects ("things") through wireless and wired connections and unique addressing schemes and create a pervasive environment where a person can interact at any time with the digital world and physical world. As shown in Fig. 2.1 IoT is collection of 6A that are Any Time, Any Where, Any One, Any Thing, Any Service, Any Path. . First, IoT is comprised of resource constrained devices, where the resources include CPU, memory, and a battery. The devices are divided into three classes according to their resource constraints [8].

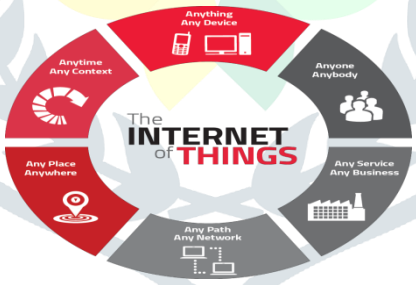


Figure1: Internet of Things [7].

1.2 Basic concepts of Big Data.

In this modern era, a large number of partnerships, organizations and associations can assemble gigabytes or even terabytes of information which are used by clients and applications. Information can incorporate different data, for instance, which items have been looked and obtained from online stores , how area or battery condition of electric devices have changed, or various pictures and have been uploaded to the Internet by consumer . analyzing the basic data and then do processed to retrieval the information .The main reason to despite the contents of each data set, many analyzing frameworks and software's can be very general in purpose; their common challenge is how to control the huge amounts of data with security, reliably, and with appropriate performance. Some excellent computer can stack various information to their memory, yet by and large appropriation offers better answers for handle huge data indexes [11].

Now days, numerous institution are gathering, grouping, and analyzing and work on the capacious amounts of data on the network. This data is basically called as "big data". Big data is creating and working on a new generation of decision support data management. Big data gives many opportunities to the Businesses for identifying the aptitude value of this data and are putting the technologies, folk, and method in place. To deriving value from big data its use of analytics. The value which is generated from big data is useful to gathering and storing big data optimize small value. It works like data

infrastructure at this point. It must be analyzed and the results used by decision makers and organizational processes in order to generate value [11].

Data analysis conceives a huge range of algorithms concerned to data mining, machine learning, and statistical analysis. When systems are using this algorithm which has been implemented, there will be several aspects to take into account [11].

Social network data is come to passing a befitting information resource for people. How the accurate result have been came by the social network or by the massive data is very important but it is also useful to fulfill the user expectation so it is hot spot in retrieving the data field. Traditional data retrieval sorting algorithms usually integrate a diversity of sorting algorithms: the algorithm which sort the data using weight and word frequencies positions method uses relative frequencies and locations of query keywords appearing in the search results for scoring[11].

In the basic algorithm of data retrieval sorting, but also based retrieval sorting scoring formulas; Direct Hit algorithms focus on directed data characteristic and feedback which are given by the people, and its idea is to track and count the timing by the user click behavior on each search result. Fetching the information becomes mostly popular for the people because it gives lots of basic idea and information in myriad number difficult situation. When people are in confusion they always suffer the net to get the answer and within few times they can get answer, as the most important tool, retrieval systems, such as search engines, have penetrated into all aspects of people's lives. Furthermore, output is obtained by a simple query which only a small part is valuable for users. Therefore, impressive modes and tools to ascertain users manage the retrieval results and make ajudicious sort are new challenges against the retrieval systems[11].

1.3 Basic concepts of Location Privacy Protection.

Location privacy is an important part of privacy protection of the Internet of Things. It mainly refers to the location privacy of each node in the Internet of Things and the location privacy of the Internet of Things in providing various location services, especially including the RFID reader location privacy RFID user location privacy, sensor Node location privacy, and location-based privacy issues based on location services[1].

Usually, data collected, aggregated and transmitted in sensor networks contain personal and sensitive information, which directly or indirectly reveals the condition of a person. If the data cannot be properly preserved, once exposed to the public, the privacy will be destroyed. Therefore, protecting the privacy of sensitive data is greatly important [14].

Location data implies moving objects, spatial coordinates, current time, and unique features different from other data, which is discrete and of high value. Before the concept of big data, most of the privacy protection methods focus on a small number of non-positional data. There are some limitations for the protection of location data privacy in big data. There are two main reasons as follows: (1) Multiple data fusion by big data makes traditional anonymity, and fuzzification technology difficult to take effect in location privacy protection; (2) Traditional cryptography technology takes little effect on the real-time analysis required by big data[23].

In summary, location privacy protection faces great challenges for big data in IoT. Therefore, we propose a location privacy protection method based on differential privacy strategy for big data in sensor networks.

II. RELATED WORK

According to this paper, devices in the internet of things generate process and exchange large amount of security and safety critical data as well as privacy sensitive information. The privacy threats of industrial internets of things can be simply divided into two categories: Privacy threats based on data and privacy threats on location. In this location privacy is important part of privacy protection of the Internet of things. It mainly refers to the location of each node in the internet of things. In this paper, they propose a location privacy protection method those satisfying differential privacy constraints to protect location data privacy and maximize the utility of data and algorithm in Internet of Things. Here they combine the utility with privacy and build a multi level location information tree model. They add the Laplace scheme to add noises to accessing the frequency of selecting data. It is more effective in protecting the privacy of data in maintaining high availability of data and algorithm. The proposed algorithm is more rigorous and has higher algorithm utility and processing efficiency [1].

According to this paper, we have studied the problem of discovering the top-k frequent patterns in a framework of differential privacy. We first proposed a novel algorithm DFP-Growth for mining the top-k frequent patterns, and proved that our methods satisfied deferential privacy. Then based on constrained in- ference technique, we proposed an efficient post-processing method for boosting the accuracy of the returned noisy sup- port counts. Experiments on real datasets show that our methods are electives in improving the accuracy, and are better than the existing solutions [2].

In this paper we theoretically prove that the proposed method is (λ,δ)-useful and differentially private. To boost the accuracy of the returned noisy support counts, we take consistency constraints into account to conduct constrained inference in the post-processing step. Extensive experiments, using several real datasets, confirm that our algorithm generates highly accurate noisy support counts and top-k Method[2].

According to this paper, Internet of Things in exchange of sensitive information raises severe privacy concerns. The Laplace mechanism – adding Laplace-distributed artificial noise to sensitive data – is one of the widely used methods of providing privacy guarantees within the framework of differential privacy. Laplace mechanism and Exponential mechanism are two of the most basic implementation mechanisms of differential privacy protection. So here read how to combine two mechanisms. The Laplace mechanism is used to add the noise that obeys the Laplace distribution to realize the differential privacy. Assuming the privacy protection algorithm f based on the Laplace mechanism, the noise keeps to the Laplace distribution with the variance and

According to this paper, Differential privacy is a formal mathematical standard for quantifying the degree of that individual privacy in a statistical database is preserved. To guarantee differential privacy, a typical method is adding random noise to

the original data for data release. In this paper, we investigate the conditions of differential privacy considering the general random noise adding mechanism, and then apply the obtained results for privacy analysis of the privacy-preserving consensus algorithm. Specifically, we obtain a necessary and sufficient condition of -differential privacy, and the sufficient conditions of differential privacy. We apply them to analyze various random noises. For the special cases with known results, our theory matches with the literature; for other cases that are unknown, our approach provides a simple and effective tool for differential privacy analysis. Applying the obtained theory, on privacy-preserving consensus algorithms, it is proved that the average consensus and differential privacy cannot be guaranteed simultaneously by any privacy-preserving consensus algorithm[5].

According to this paper, The Internet of Things and big data represent an explosion of information creation, sharing, and use. This is due to greatly increased types and numbers of connected physical devices such as sensors and actuators, and systems such as social networks used by people. Because location information is a large component of IoT information, and concerns about its privacy are critical to widespread adoption and confidence, location privacy issues must be effectively addressed. It is hoped that the framework presented here, which looks at six phases of location information flow in the IoT and three areas of privacy controls that may be considered to manage those flows, will be helpful to practitioners and researchers when evaluating the issues involved as the technology advances. Here refer basic concept of location privacy of large data in internet of things [6].

III. EXISTING SYSTEM

3.1 Existing System working Process.

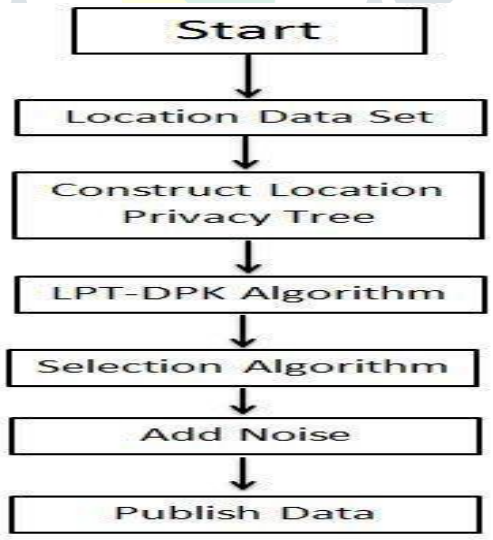


Figure2: Existing System Working flow chart.

3.2 Proposed System working Process

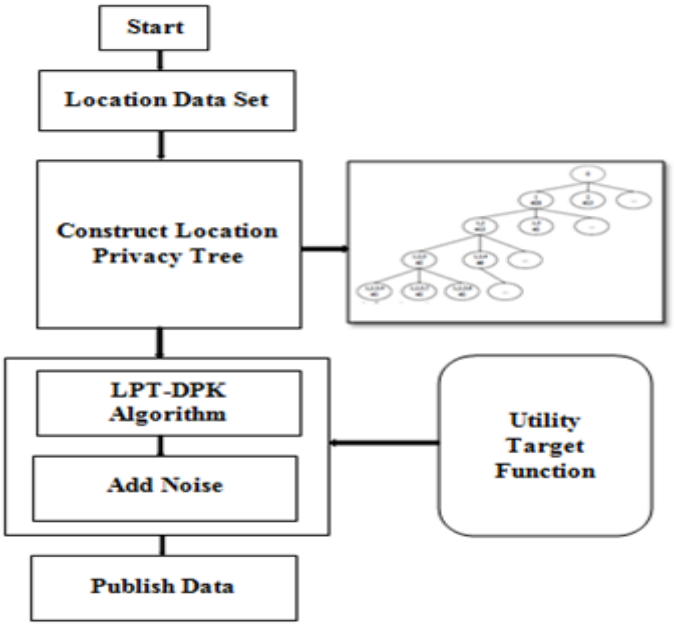


Figure3: Proposed System Working flow chart.

3.3 Collect Location Data set

Table 1 - Location Correspondence

Number	Location Information	Accessing count
1	Computer Building	28
2	Remote sensing unit	13
3	library	2
4	Management center	6
5	Training gym	5
6	Sport compound	30

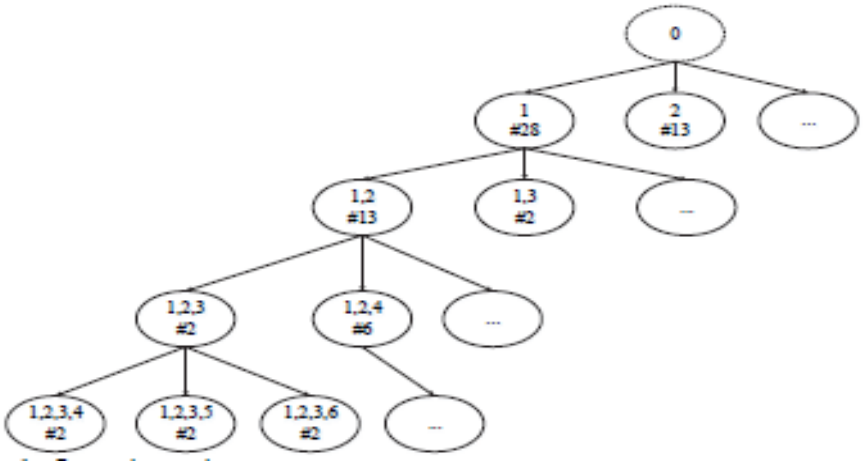
Table 2 - Location Data Information

Number	Location label	Accessing count
1-28	1	28
29-41	2	13
42-43	3	2
44-49	4	6
50-54	5	5
55-84	6	30
85-97	1,2	13

3.3 Construct Location Tree

According to the table -3 , we can construct the location privacy tree like figure 4.

Figure 4-Location Privacy Tree



3.5 LPT-DP-K algorithm

Firstly, we choose the location privacy tree construct and maintain the relation among the location data. Secondly, we select the sensitive location information which is most likely to disclose privacy to add noise. The algorithm summarizes as follows [1].

- **In LPT-DP-K algorithm P(a) Equations :-**

$$P(a) = \frac{ai.w}{\sum_{j=1}^{n} aj.w}$$

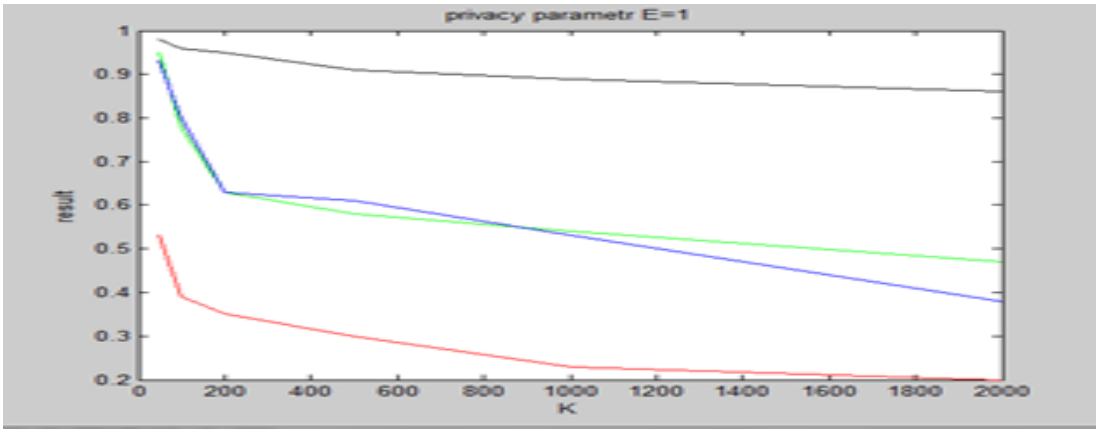
- **Utility Target Function apply in Probability P(a).**

$$P(a) = w1.U1(CA) + w2.U2(DA) + \cdots$$

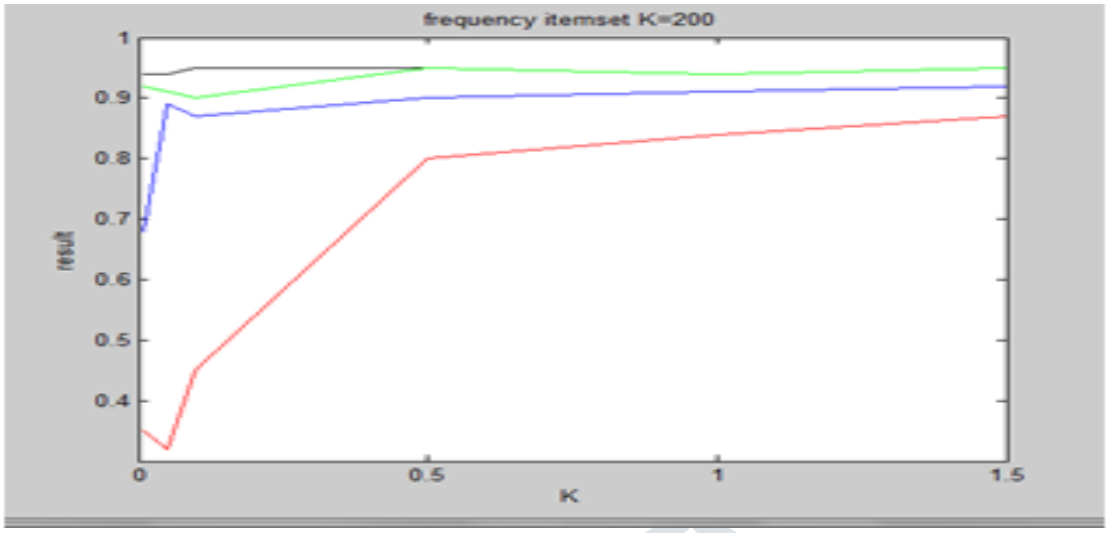
This is Utility Target Function for probability equation[20]. Here 'a' is data set patterns and 'w1,w2,w3' is weight of patterns. CA- attack cost ,DA – Technical Difficulty

IV. RESULT ANALYSIS OF ACCURACY

1.Privacy Parameter E =1,
Frequent Itemset K(50,100,200,500,1000,2000)



2. Frequent Itemset K= 200,
Privacy Parameter E (0.01,0.05,0.1,0.5,1,1.5).



IV. CONCLUSION

Location privacy protection can be archive using Location privacy tree, LPT-DP-K algorithm, Selection algorithm and Laplace noise algorithm. In the next steps explore the more efficient data structure to express location information in the process of location data expression and propose more utility target functions. Main objective is to plug utility target function in our work to increase privacy of location data. Another objective is use to get high availability and low density.

REFERENCES

[1] Chunyong Yin, Jinwen Xi, Ruxia Sun, Jin Wang. "Location Privacy Protection based on Differential Privacy Strategy for Big Data in Industrial Internet-of-Things " - IEEE, 2017.

[2] XiaojianZHANG,Xiaofnf MENG " Discovering top-k patterns with deferential privacy–an accurate approach " Springer 2017**.**

[3] FragkiskosKoufogiannis, Shuo Han, George J. Pappas "Optimality of the Laplace Mechanism in Differential Privacy " Cornelluniversity library paper (source google scholar)-2015.

[4]Yang D. Li, Zhenjie Zhang, Marianne Winslett,Yin Yang "Compressive Mechanism: Utilizing Sparse Representation in Differential Privacy " : ACM – 2011

[5]Jianping He and Lin Cai."Differential Private Noise Adding Mechanism and Its Application onConsensus." Cornell university librarypaper (source google scholar)-2017.

[6] Robert P. Minch. "Location Privacy in the Era of the Internet of Things and Big Data Analytics"- Hawaii International Conference on System Sciences-2015.

[7] https://www.agtinternational.com/wp-content/uploads/2013/11/IoT1.png [Accessed OCT 2015]

[8] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, Hui-Ying Du, "Research on the architecture ofInternet of Thing" 3rd International Conference in IEEE Conference Publications ICACTE 2010.

[9] P. Gupta and G. P. Bhattacharjee, "A parallel selection algorithm," BIT, vol. 24, no. 3, pp. 274–287, 1984.

[10] I.F. Akyildiz, W.su,Y. Sunskarasubhramaniam."Wireless Network Sensor Network" ComputerNetwork the International Journal of Computer and Telecommunication Networking ,vol:-13, no.4-2010.

[11]NikunjSoni, BintuKadiwala," Big data security and privacy issues -A survey" Innovations inPower and Advanced Computing Technologies (i-PACT)-2017.

[12]KoheiKasori Fumiaki Sato,"Location Privacy Protection Considering the LocationSafety".IEEE-2015.

[13]Kiran Mehta, Donggang Liu, Matthew Wright "Location Privacy in Sensor Networks Against aGlobal Eavesdropper" International Conference in IEEE Conference Publications ICACTE 2007.

[14] Imran Memon," Authentication User's Privacy: An Integrating Location Privacy Protection Algorithm for Secure Moving Objects in Location Based Services" Springer Science+Business Media New York 2015

[15] Marius Wernke, PavelSkvortsov, Frank Durr, Kurt Rothermel ,"A classification of locationprivacy attacks and approaches". Springer-2012.

[16]JieBao, Yu Zheng ,Mohamed F. Mokbel "Location-based and Preference-AwareRecommendation Using Sparse Geo-Social Networking Data".ACM -2012.

[17] Gang Sun, Victor Chang, MuthuRamachandran, Zhili Sun, Gangmin Li, Hongfang Yu and DanLiao, Efficient Location Privacy Algorithm for Internet of Things (IoT) Services and Applications, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2016.10.011.

[18] K Mivule –"Utilizing noise addition for data privacy" arXiv preprint arXiv:1309.3958, 2013 - arxiv.org

[19]Li, Yaping, et al. "Enabling multilevel trust in privacy preserving data mining." IEEE Transactions on Knowledge and Data Engineering 24.9 (2012): 1598-1612.

[20] Liu, Hai, et al. "Adaptive Gaussian Mechanism Based on Expected Data Utility under Conditional Filtering Noise." KSII Transactions on Internet & Information Systems 12.7 (2018).

PATENTS

[21] Michael R.gardner,WayneW.Ballantyne,Zaffer S. Merchant for "SYSTEMAND METHOD FOR E911 LOCATION PRIVACY PROTECTION-US7751826B2,2010.

[22] Bennie L. Farmer, Ann Arbor, MI for "SYSTEMS, METHODS, AND COMPUTER PROGRAM PRODUCTS FOR PRIVACY PROTECTION" US 2003/0130893 A1,2003.

BOOKS

[23] Ruben Rios, Javier Lopez, Jorge Cuellar;1stEdition;Location Privacy in Wireless Sensor Networks,CRC Press,2016 .

THESIS

[24] Shuo Wang,PhD Thesis "Exploration and protection of Location Privacy in online social networks"2018.

[25] Damien schorer, PhD Thesis "Privacy in the Internet of Things era"2016.