The Ethics Issues of Location-Based Services on Big Data and IoT

Victor Chang[1], Yeqing Mou[2] and Qianwen Ariel Xu[1, 2]
[1] School of Computing, Engineering and Digital Technologies, Teesside University, UK
[2] International Business School of Suzhou, Xi'an Jiaotong-Liverpool University, Suzhou, China
ic.victor.chang@gmail.com, a549844259@qq.com and iamarielxu@163.com

Abstract. Both Internet of Things (IoT) and big data are hot topics in recent years. They indeed have brought about the change of business, promoted the progress of science and technology, and facilitated the lives of human beings. IoT creates the opportunity to connect every item to the internet and Countless science and technology have supported the achievement of this goal. LBS is one of the indispensable technologies. It brings significant benefits to the business community, the individual, the society and the national defense. However, at the same time, an individual's personal information is disclosed and even attacked by 'information thieves. An inevitable reality is that the prerequisite of getting a location service is to expose your position first. Therefore, the privacy-related ethics issues are generated, and the danger is imminent, although there are corresponding protective measures.

Keywords: Location-Based Services (LBS), Big Data, IoT, Ethical issues and challenges

1 Introduction

In the Internet of Things (IoT) environment, everything could be connected by the internet. IoT refers to the kind of internet-based expanded network. Besides, the extended client-side exchange information with each other and communicate between any objects and items. The data and information could be exchanged among different devices, such as between different smartphones, which not only improves the convenience of life but also causes some data-related problems violating ethics. As an essential component of IoT, Location-based Services (LBS) become the services provider as well as the 'arch-criminal' of information leaks. Based on the internet of things, the LBS system can collect and convey all kinds of situational perceived data flexibly and efficiently through the perceived interaction between physical space and information space. The LBS system based on IoT will provide users with the customizable personalized real-time location service by processing the collected perceived information intelligently. It is undeniable that LBS, based on IoT, brings attractive services to people. However, at the same time, it also brings dangers about disclosure of personal information. This type of information often contains both the user's sensitive information, such as habits, health status, social relationships, and even identification. This paper will be divided into five parts to illustrate the situation of the application of LBS based on big data and IoT background and provide some solutions.

2 Big Data and IoT

2.1 Big data

Big Data is an emerging term that describes the surprisingly rapid proliferation in the volume of data in structured and unstructured form Stergiou and Psannis [1]. According to Stergiou, et al. [2], more trusted decisions are made based on accurate big data, greater operational efficiency cost reduction and reduced risk resulting from better decisions. In the internet of things environment, the data acquisition capability of various sensors, such as smartphones and wearable computing devices, has been improved significantly. With the development of IoT, cloud computing and other related technologies, every change in our behavior, location, and even body physiology data is sunk for the kind data which could be recorded and analyzed [3]. Besides, the concept of "big data" is generated with the advent of the wide application of the internet. The number of Internet users, including individuals, enterprises, and institutions, increases sharply, making it relatively effortless to access and share data. Users can easily access the data by network and massive data is created with user's internet habits. For example, through intentional or unintentional sharing, clicks, and browsing, these operations quickly provide a large amount of data. Unlike the previous massive data concept, the emerging conception, 'big data', has four

unique features, volume, variety, velocity, and veracity [4]. Variety refers to the multiform sources of data and various existing forms of information. For example, social media provide an enormous amount of users' location and life condition information. Vehicle navigation record a large number of driving trajectory information. Velocity means the value of the data will be depreciated—the development of a traffic query system dependent on the velocity [4]. The location of big data collected through LBS also has these four features.

2.2 IoT

With the emerging IoT era, every object could be equipped with a smart device to collect data through the internet. The challenge for personal privacy and data is generated with the development of IoT. Rivera and van der Meulen [5] predicted that a $14 billion economic influence is expected to be created due to IoT by 2022. The sensors, a crucial technology of IoT, is used to collect transmit data to the internet and achieve 'everything is connected'. According to Caron et al.[6], IoT might strongly impact personal privacy when more data with different sources are collected using these sensors.

3 LBS and LBS applications

3.1 The principle of LBS

LBS, Location-based Service, refers to a collection of location-related services based on the location information of users. There are two technologies to access location information of mobile terminal users and provide location services for them. They are the radio communication network operated by telecom or mobile, such as GSM and CDMA and external positioning technology, such as GPS. Besides, a kind of value-added service provides the corresponding services for users with the support of the GIS (Geographic Information System) platform. In a word, LBS consists of three kinds of technologies, GPS, base station and GIS.

GPS is just one of the most common components of LBS to provide location service for outdoor users. The application of GPS can be divided into two aspects, military and civil. In the context of the IoT, GPS is a vital component of Location-based services in the civil field. In terms of GIS, there are many elementary differences between LBS and GIS, although many of the functions in LBS are similar to those of traditional GIS systems. GIS system could usually make use of significant computing resources to provide professional geographic data analysis and processing for a small number of technicians.

On the contrary, LBS provides limited geographic data services to a large number of ordinary users and these services run on mobile terminals with limited resources. According to Zhou et al. [7], the LBS service providers usually possess these characteristics: high-performance, expansibility and instantaneity, etc. These properties allow LBS to provide location services based on big data. Taking high-performance and expansibility as an example allows LBS to process the massive user query requests to decrease time waiting [8].

3.2 The application of LBS

LBS has become the current application and research hotspot. Whether it is a public user or an industry user, there is a wide range of needs for access to locations and related services. The early LBS system was mainly used to quickly locate the caller's location in an emergency to implement rescue activities. At present, LBS has been widely used in military, transportation, logistics, medical, people's livelihood and so forth.

The specific application of these location-based services can be divided into four categories, trigger services, information services, tracking service and assistance [9]. The LBS information service and tracking focus on providing location services for users on social media platforms. Taking navigation software as an example, navigation software, such as Baidu Mapping, can provide real-time information about road conditions and plan optimal travel routes for users. Additionally, drivers could find the nearest gas station with the help of these services. Besides, in a large museum (such as the Forbidden City

Museum), visitors can enjoy the explanation of each collection through location-aware voice guider with the tracking service [7].

These applications of LBS created values to two groups, business and individuals, in the IoT environment. On the one hand, LBS changed how business works. As for the vehicle insurance company, their development benefits from LBS services because they could plan the insurance solutions that are most beneficial to the interests of the company with the help of LBS. It could record the trajectory information, such as the common driving locations and paths of every insured vehicle, analyze the risk levels, and then custom car insurance prices for different insurants [10]. As for the transport company, LBS applications help them plan the optimal driving route with the lowest fuel costs and breakdown cost [10]. Then, LBS realizes the accurate marketing of the service industry. For example, a restaurant could provide the best recommendation for users initiatively, accurately and duly by establishing the cooperation with map software because LBS records where users are and even analysis what they want through the users' query.

On the other hand, individuals indeed enjoy the kind of data-based position services. Firstly, customer experience on social media platforms is improved since LBS records user-generated locational data and transform it into the available information. Social media platforms of mobile internet terminal offer a wide range of location services to users. It helps individuals create closer connections with the outside world and enhance the relevance between social networks and geographic locations. For example, individuals could share their location information with their friends on Weibo, WeChat, Facebook, and other social media platforms, bringing convenience to our lives. Then, vehicle navigation is one of the most widely used areas of LBS. With the application of vehicle navigation, self-driving tours meet individuals' needs for a journey. LBS not only provides navigation information services for drivers but also offers information about the nearby tourist attractions. Users could send a query about fining the nearby tourist attractions information, and then they could receive a large number of traveling strategies. As for the bus and taxi, LBS achieves the Intelligence of transportation, including smart bus and smart taxi. For instance, the public transport dispatching monitoring and management system could generate the optimal driving route for buses base on the real-time location information. Besides, it could issue the scheduling instruction, such as acceleration, bypass and departure, etc., to these public vehicles according to the driving condition set in advance in the database. Finally, the wearable devices are also the kind of LBS application. The smartwatch, smart bracelet and even the positioning chip embedded in sneakers are used to provide location services for customers. They can collect the outdoor sports route and generate images to record the exercise process.

4 Ethics issues

4.1 Ethics Issues

The research opportunities of LBS brought about a number of research challenges on theory, technology, and ethics. For example, the types of big data are usually diverse, unstructured and multidimensional. Effective representation models and processing technologies are required to organize and analyze these data more efficiently and effectively [11]. In addition, all the services mentioned above are based on the location information from users. The ethics issue is related to the usage of this information. If used to analyze the query from users only, then the ethics problem is not worth raising concerns. However, if hackers or other people want to earn immoral and illegal gains from the data stream, there are serious ethical issues related to privacy for individuals. Location privacy is location information from the IoT users, one of the essential elements for IoT to perceive information and the prerequisite for IoT to provide location-based service with users. As for privacy, it is defined as the kind of information that the users are unwilling to expose. Therefore, it is unethical and even illegal to access and analyze user data without permission. Privacy is the right of citizens to their own privacy, the core of which is to control their own privacy according to their own will. Unauthorized positioning, location disclosure, mandatory commercial infringement, unreasonable use will harm the user's interests. For this reason, some users tend not to provide their information to the LBS providers, leading to insufficient data for LBS applications. Zhang et al. [12] tried to deal with this problem from a technology perspective. They proposed an algorithm established on the k-anonymity criterion to generate dummy locations and defined

the trajectory entropy as a new variable to evaluate the performance of anonymity. Their simulation showed excellent performance. Different from them, this paper tends to focus on detailed ethical issues.

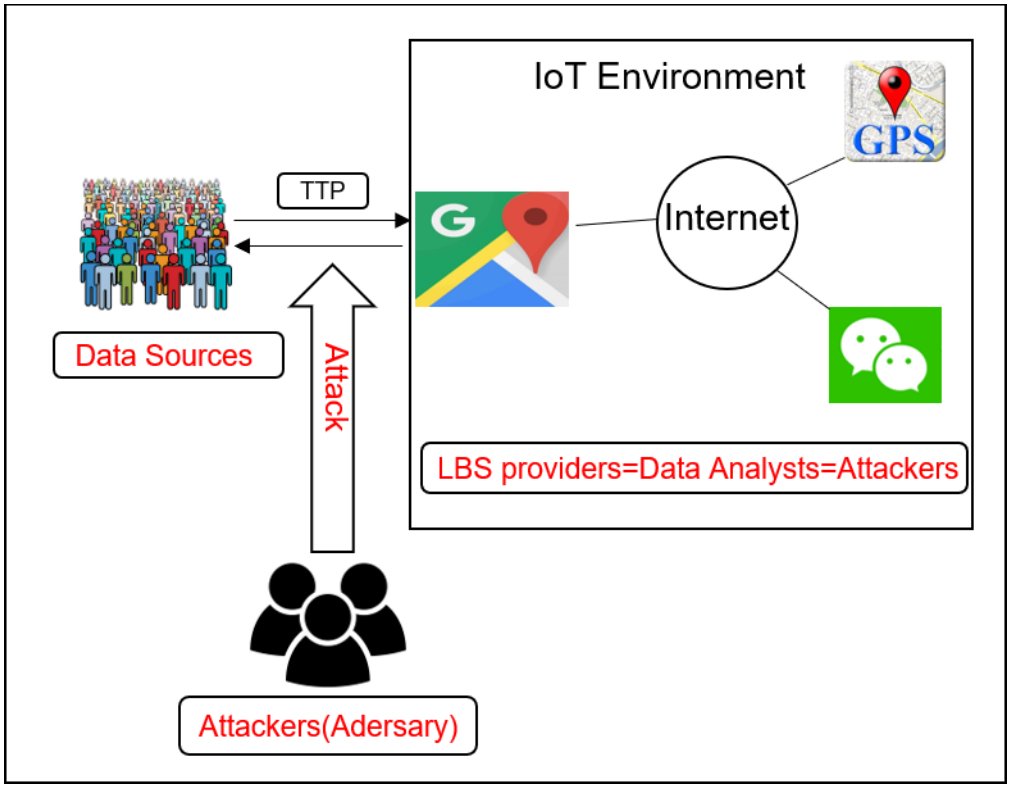

Figure 1. Ethical issues based on LBS.

Figure 1 exemplifies the relationship between data analysis and ethical issues based on LBS. It is obvious that the source of data is used and the data could be analyzed by LBS providers to improve the location services. However, the data also could be attacked by both adversary and LBS providers. The former could attack the defense mechanism, such as TTP(Third-Trusted-Group), to access the database and analyze the user's personal information. As for the latter, they have the authority to obtain user data. Even though the data are not exact, LBS providers still could analyze more information by combining all queries or employing other methods.

4.2 Potential Privacy Disclosure Issues

It is undeniable that the downside always arises with the benefits. From the view of ethics, the drawbacks are the kind of threats related to privacy for users. It is effortless to infer the privacy information and even sensitive information, such as social status and users' health condition by analyzing their location information since the prerequisite to enjoy location services is to deliver the location information.

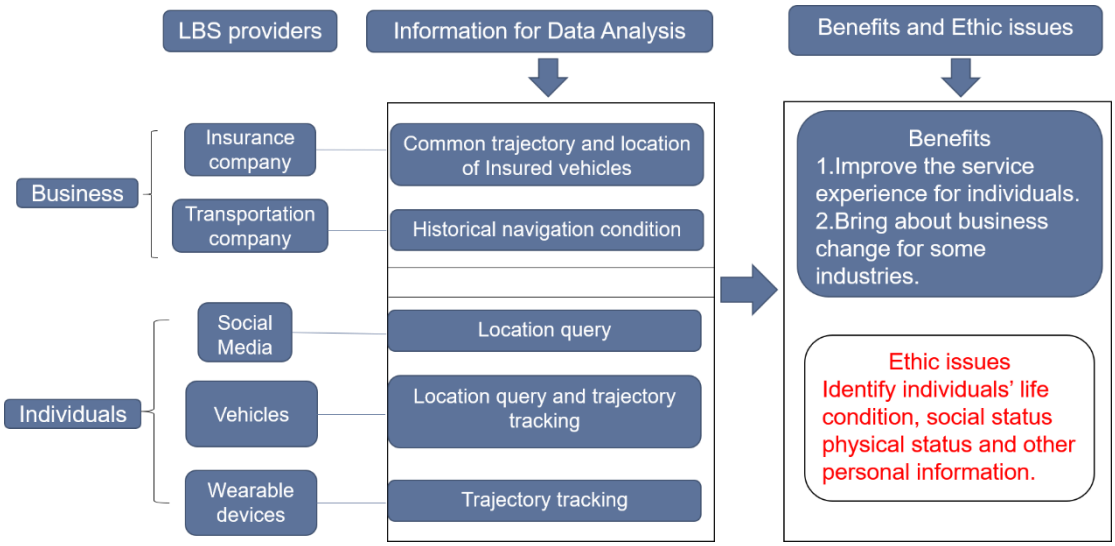

Figure 2. Benefits and privacy problems with data analysis

Figure 2 shows the information used for data analysis and the benefits and privacy problems generated with the data analysis. The social media application is one of the most popular application areas of LBS and recent research outputs show that the privacy issues caused by social media cannot be ignored. Vicente et al. [13] revealed two kinds of threatens from the social media platform: sensitive privacy and re-identification. Besides, researchers, Li et al., explained that contextual information makes it is easier to achieve re-identification [14]. For example, an adversary could keep tracking users' trajectory in real-time through free software, such as Google Maps, and freely available data sources such as the Twitter stream data [14]. Then, they combine and analyze these data from two sources to identify an individual's life condition. Furthermore, Wang et al. [15] mentioned that when the users issue the location information on the social media platform, metadata tends to be revealed without the user's permission and they even may be unaware of it if the location-based service on users' phone is in the active condition. The data thieves can access to these metadata to identify individuals and their moving tracks directly.

In fact, these metadata exposed individuals' information and used to improve the service provided for themselves. Taking Twitter as an example, there are more than 500 million tweets on twitter platform and they are used to enrich a wide range of geospatial target analysis. This is why users could receive recommendations for restaurants or the prompt about nearby friends [15]. Additionally, there is a similar danger to privacy in the domestic market. Taking WeChat as an example, its built-in programs, such as nearby people, shake it up and WeChat sports also involve infringement of privacy through location services. User avatars, personal data, and other information will be seen by people nearby through the 'People nearby' program. Furthermore, the exact distance from the nearby person to your location will also be displayed. Zhao [16] also revealed that WeChat accesses user location information indirectly through the leaderboard on WeChat sports. Although users could empty the location information so that the information is not available to the other users, backstage will still record it for big data analytics [16]. Secondly, as for the vehicles with the LBS, it provides the optimal route for drivers.

However, at the same time, users' related information is recorded by LBS. This information includes the life condition of users and their identification as well as social status. For example, LBS could infer the individuals' addresses of home and company by analyzing the most common query on the navigation software. Combined with other query information, such as the grade of the most frequented restaurant, the LBS can even infer the standard of living and consumption-ability of the person who sends a query. This information could be accessed by car compass as well as navigation software on smartphones. Finally, as for the wearable devices, there are also some ethical issues related to owners' privacy. Take smart bracelets as an example; these bracelets record runners' physical condition information by analyzing their heart rate and other indexes. It is undeniable that the authorities can analyze bracelets' physical status based on the health information from their smart bracelet records, however, if they are trafficked to the healthcare industry, customers will receive unnecessary medical marketing ads.

What is more worrying is that the physical condition is more valuable than common people, possibly leading to the formation of the information trafficking industry if the authorities neglect to supervise [10]. These ethical issues are not only immoral but also even illegal. The privacy trafficking industry is a potential danger caused by LBS. Once this trade is generated, then users' information, especially the celebrity's information, will be the source of illegal gains. The situational context data of LBS service in IoT space not only contains personal privacy information such as user identity, bank account, current location, activity trajectory, behavior mode, living habits, etc. but also may involve business secrets such as marketing plan, product information, customer information and so on. Lu and Liao [17] point out that business secrets are more likely to cause crime.

Compared with the previous LBS system, the LBS system in the IoT space faces more serious privacy and security problems. Suppose the privacy and security of LBS services in the IoT space cannot be guaranteed. In that case, the popularity of LBS services in personal applications and the large-scale promotion of the commercial sector will be seriously affected [17].

5 Recommendation and Discussion

5.1 Existing protection method and the weakness

Figure 3. TTP-based scheme

There is a collection of methods and techniques to solve these location-related privacy issues while they are defective. Most location privacy protection solutions can be categorized into two architectures, TTP-based schemes and (ii) TTP-free schemes. Figure 5.1 illustrates that, under the TTP-based scheme, TTP is responsible for receiving and transforming user location information and query, and then sending it to lbs. LBS can only deal with the query based on imprecise location information and then return the results to the user via TTP. For example, the most common method is the cloaking technique, which is based on the K-anonymity model. K ensures that the query from one user is mixed with at least K candidates and K is the most significant risk information disclosure. The queries will be sent into the centralized location anonymizer and then the queries will be generated into a bigger cloaking region to mix these queries. Finally, these cloaking location queries rather than the exact one will be sent from anonymizer to the location-based services devices [18], which guarantee that the attacker cannot identify private information belongs to which specific individuals. As for this technique, the most important as well as the weakest segment is the cloaking area. If the adversary attacks this area, all information will be revealed because all locations are anonymized [19]. A relatively more advanced technique is 'dummy location'. However, the side information of this technique is neglected and it is easy to be attacked by adversaries, then it is neither not functional [18]. Furthermore, the protocol about privacy-preserving is also a popular method [20]. However, the drawback of it is that the service provider cannot predict all purposes.

What is more, it is meaningless to tell the uses of what they will do with this location information because it will make the location data become biased and not truth [3]. Apart from these vulnerabilities, there also other doubts about these protection methods. He et al. [21] revealed that the surrounding physical environment fundamentally limits privacy protection. Jiang et al. [22] found that the continuous LBS queries are ignored because the previous protection method only deals with snapshot user locations, one-time queries for the K-anonymity. In conclusion, the trusted third party is a bottleneck in computing and communication in the whole system. The low success rate for anonymity, the high cost of communication, and the weak ability are also drawbacks to resisting attacks from adversaries.

5.2 Recommendation

The drawbacks of these existing methods are innumerable. 'The biggest challenge is how to balance individual privacy while still making the individual's location data publicly available for mining and analysis'[15]. Users' information is not only helpful for the business and individuals themselves but also practical for authorities. From real-time universal health monitoring for people to future urban planning, large amounts of data are needed. It would generate great benefit to users if researchers and government agencies access this information and use it for research. Therefore, it is crucial to balance their relationship.

When the user wants to get the efficient and convenient location service, their clear text information can easily become the attacker's attack objects. According to Yan et al. [8], today, many LBS providers abroad pay the growing attention to user data confidentiality, such as

- binding users to hardware uniquely to avoid situations where multiple users are on the same device,
- increasing user behavior management, identifying suspicious user groups or user behavior, and
- providing real-time alerts based on customized policies.

However, few of these app developers or operators at the domestic are concerned. Therefore, supervisors need to do more to strengthen the regulation of consulting privacy on a social level. From a technical point of view, Yan et al. [8] point out that two kinds of recognition abilities should be improved for the LBS providers. On the one hand, it is necessary to enhance user recognition ability and make it is difficult for non-real users to access real data. On the other hand, improving the hardware recognition capabilities for mobile devices and developing corresponding security policies for relevant tools such as simulators are essential. Besides, since the principle of location-based services, the biggest contradiction is that the higher the quality of location-based service, the higher the risk of privacy leakage.

According to Zhou, et al. [7], the goal of most current research revolves around the "relative privacy" protection of the location, or "controllable privacy," where location information is released in a form that is relatively difficult for attackers to identify. This form could meet the user's personalized privacy needs and ensure that LBS can obtain the location even though it cannot access the location information [7]. Besides, the three biggest challenges to break the existing methods are as following. The first one is about the measurement standards of the extent of user privacy leaks. Then the second one is how to be responsible for the comprehensive protection for data-based location privacy. The last one is how to trade-off between privacy protection and the availability of these location services. The traditional technique, such as K-anonymity, does not consider how to measure the degree of a privacy breach or protect users' privation completely, let alone balance them.

6 Conclusion

Along with the development of big data mining and analysis technology, in the IoT environment, all groups are experiencing and enjoying the convenience that LBS brought to all aspects of social development, such as military, commercial and personal life. In the business world, LBS has brought about substantial business changes. For example, the transportation industry could compute cost-optimal routes for the future transportation plan by analyzing historic navigation records. For individuals, everyone lives in the services provided by LBS since all query content sent by the user are the best source of data analysis for the LBS providers. However, the contradiction is that the high quality of LBS is based on the extent of the exposed location information and fragile protection mechanisms. Therefore, whether it is for LBS providers, government regulators, or individual users, it is essential to raise personal information protection awareness. For the first two groups, it is urgent to find a breakthrough to protect user privacy information and find a definition of privacy.

Acknowledgment

This work is supported by VC Research (VCR 0000082).

References

[1]. Stergiou, C. & Psannis, K. E., 2017. Efficient and secure BIG data delivery in Cloud Computing. Springer, Multimed Tools Applications, 4, pp. 1-20.

[2]. Stergiou, C., Psannis, K. E., Gupta, B. B. & Ishibashi, Y., 2018. Security, Privacy and Efficiency of Sustainable Cloud Computing for Big Data and IoT. Sustainable Computing: Informatics and Systems.

[3]. Mayer-Schönberger, V. & Cukier, K., 2013. The Age of Big Data. s.l.:Zhe Jiang People Publishing House.

[4]. Ma, H., 2014. Haixiang Ma Blog. [Online] Available at: http://www.mahaixiang.cn/sjfx/803.html [Accessed 10 12 2018].

[5]. Rivera, J. & van der Meulen, R., 2014. Gartner. [Online] Available at: https://www.gartner.com/newsroom/id/2819918 [Accessed 06 12 2018].

[6]. Caron, X., Bosua, R., Maynard, S. B. & Ahmad, A., 2016. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer law $security review, pp. 4-16.

[7]. Zhou, A., Yang, B., Jin, C. & Ma, q., 2011. Location-Based Services: Architecture and Progress. CHINESE JOURNAL OF COMPUTERS, 7, 34(7), pp. 1155-1571.

[8]. Yan, D., Wang, Y., Xue, Z. & Hu, L., 2016. Research on the security risk of APP data for LBS service. Communications Technology, 12, 49(12), pp. 1702-1708.

[9]. Sheng, X., 2012. LBS- Application of technology in social media. Friend of Science, 2012(2), pp. 159-161.

[10]. Wang, L. & Meng, X., 2014. Location privacy preservation in big data era: A survey. Ruan Jian Xue Bao/Journal of Software, 25(4), pp. 639-712.

[11]. Yao, X. A., Huang, H., Jiang, B., & Krisp, J. M. (2019). *Representation and analytical models for location-based big data. International Journal of Geographical Information Science,* 33(4), 707-713. doi:10.1080/13658816.2018.1562068

[12]. Zhang. L, Qian. Y, Ding. Ma. M, C., Li. J and Shaham. S. (2019). "Location Privacy Preservation Based on Continuous Queries for Location-Based Services," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 1-6.

[13]. Vicente, C. R., Freni, D., Bettini, C. & Jensen, C. S., 2011. Location-Related Privacy in GEO-Social Networks. Internet Computing, 15(3), pp. 20-27.

[14]. Ajayakumar, J. & Ghazinour, K., 2017. I am at home: Spatial Privacy Concerns with Social Media Check-ins. ScienceDirect, 08, pp. 551-558.

[15]. Wang, S., Sinnott, R. & Nepal, S., 2016. Protecting the Location Privacy of Mobile Social Media Users. International Conference on Big Data (Big Data), 7, 978(1), pp. 1143-1150.

[16]. Zhao, C., 2017. The privacy protection dilemma of social media in the new media era-taking WeChat as an example. THEORY RESEARCH, 2017(12), pp. 5-6.

[17]. Lu, H. & Liao, l., 2014. Privacy-preserving model of LBS in Internet of Things. Computer Engineering and, 50(15), pp. 91-96.

[18]. Sun, G. et al., 2017. Efficient location privacy algorithm for Internet of Things (IoT) services and. Journal of Network and Computer Applications, pp. 3-13.

[19]. Zhao, H., Yi, X. & Wan, J., 2016. Privacy-area Aware All-dummy-based Location Privacy Algorithms. Proceedings of the IEEE First International Conference on Mobile Service, pp. 9-16.

[20]. Li, X. & Jung, T., 2013. Search Me If You Can: Privacy-preserving Location Query Service. 2013 Proceedings IEEE INFOCOM, pp. 2760-2768.

[21]. He, X., Jin, R. & Dai, H., 2018. Leveraging Spatial Diversity for Privacy-Aware. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 6, 13(6), pp. 1524-1534.

[22]. Jiang, H., Zhao, P. & Wang, C., n.d. RobLoP: Towards Robust Privacy Preserving Against Location Dependent Attacks in Continuous LBS Queries. IEEE/ACM TRANSACTIONS ON NETWORKING.