DOI: http://dx.doi.org/10.26483/ijarcs.v10i2.6400

ISSN No. 0976-5697

Volume 10, No. 2, March-April 2019

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

PRIVACY PROVISION FOR TIP ATTRIBUTES IN NTTP BASED LBS SYSTEMS

Syeda Aniqa Bukhari
Department of Computer Science
GC Women University Sialkot
Sialkot, Pakistan

Wafa Zainab
Department of Computer Science
GC Women University Sialkot
Sialkot, Pakistan

Sheeza
Department of Computer Science
GC Women University Sialkot
Sialkot, Pakistan

M. Usman Ashraf
Department of Computer Science
GC Women University Sialkot
Sialkot, Pakistan

Abstract: Location Based Services (LBS) are mainly concerned to protect privacy of users because privacy is a core need of any user who deals with any computing system. In LBS systems, privacy is concerned with three fundamental metrics such as temporal information, user identity & spatial information. According to variance of multiple scenarios these three attributes must be protected because losing one's privacy attribute can lead to full privacy intervention of user. Different strategies are being used to deal these metrics including TTP and NTTP. Therefore the purpose is to bring the privacy at user's satisfaction level in LBS for user identity, temporal & spatial information attributes by using NTTP (Non-Trusted Third Party). In current study, we have conducted a comprehensive survey on approaches of NTTP in LBS systems. The purpose of survey was to focus on further advancements of these proposed models.

Keywords: Location Based Services (LBS); User Privacy; NTTP Approaches; Temporal Information; Spatial Information; User Identity

I. INTRODUCTION

Now a days, technology is rapidly increasing even everyone sitting at home can visit far-off places and make friends whom they never meet in real life but virtually they are connected. [25]To access any place or person, knowing location is very important, and all these communications depend upon location based services through which we think of the world as everything is on your hand. Location Based Services are based on accessing geographical location of users by their handheld devices. LBS also helps users to find out required and nearest organizations and places like banks, educational institutions, restaurants, shopping areas, businesses and nonprofit organizations and also provides different kinds of services like delivery services, advertisement services, selling services, communication services, finding location services etc. By getting user's identity, position and temporal information and we have to protect these three attributes from unauthorized use. There are few main kinds of LBS being used these days, Location Tracking services, location aware services and map & navigation services. [24]Despite of providing a lot of benefits like finding location for tourism if we are unaware of the ways, playing online games with friends at different and remote locations and social networking (For example, Facebook, Twitter, Google play store and App store where user's points of interests are got by keeping their personal information and sensitive data). [26]Google Maps using GPS (Global Positioning System) through which everyone can trace any location from anywhere and also where users personal information can be used by a third party without any permission for statistical analysis and finding typical mobility patterns and user doesn't know that who is using his data and for which purpose it's being used. All these services require our personal information due to this, user's privacy is affected. Privacy issue is that our personal information given to LBS is not completely secure still it

can be attacked by adversaries. There may be a case when we can think of giving fake identity or location to LBS for preserving privacy but if a customer orders pizza then he/she will must have to give his/her right location and also using Amazon a user must have to create an account using real information so these cases require actual information and here we encounter the problem of protecting user's real identity. [18]LBS uses two ways to provide privacy by using TTP (Trusted Third Party) and NTTP (Non-Trusted Third Party) where TTP means there is some third party like any node or server which is helping LBS to protect users. LBS using TTP fully rely on the third party but it's not sure for a third party to always be reliable for the protection of user's personal information. [11]There exist numerous approaches which are dealing with privacy preservation in context of TTP in LBS. Main approaches, six of them, are the ones dealing with concepts of Dummies, K-anonymity, Obfuscation, spatial cloaking, mix zones and Cooperation between users and Caching. But all mentioned above approaches have some serious demerits regarding privacy and security of user on LBS it is quite hard to attain a perfect approach with minimum flaws. Due to these reasons we choose NTTP for preserving privacy which is beneficial because it does not fully involve a Third Party but involves as a minor part. LBS using NTTP are somehow independent of the third party because third party can be a major source of leaking user's information if it's not trusted. There are many

proposed approaches of using NTTP in LBS some are: silent period, coordinate transformation, The L4NE protocol, Decentralization, Cache Based Approach, Optimal Mechanism, Geo Indistinguishability, Context-Aware Privacy Protection (CAP) and blind filtering[1], [2], [3], [35], [14], [23], [32], [24], [14], [17], [7], [5], [22]. All discussed in detail in section III. All these techniques help an LBS to protect user's personal information from being accessed by unauthorized access.

II. USER PRIVACY ATTRIBUTES

The attributes to be protected are the user identity, his/her spatial information (position), and temporal information (time). [18]The fortification objective of the user defines which characteristics of the information should be sheltered and which can be publicized.

A. Temporal Information

It includes time or the point in time when position of the user is correct. [29]In some situations, position information is only understood to be important if it has relationship with the temporal information. For instance, a user may want to share his information with others when he is travelling the world, Moreover, but still he does not want to disclose his speed rate to others. This means that real-time information cannot be in this situation without concerning for privacy, whereas timely delayed updates can be used to maintain the protection purpose. The user also want to hide and manage the time periods of his position or his/her actual moving path.

B. Spatial Information

[18]It defines the location of the user and makes hard to track the actual location of the user. Its main aim is to protect actual location of user from attacker.

• User can give feedback for the organization he/she just visited for example a restaurant, bank or university without disclosing his position.
• Use an improved navigation system for instantaneous jamming prediction on traffic roads.
• User does not want to display that he is in a coffee shop by posing to be in an office admin block.

C. User Identity

The purpose is to hide user identity while he is using a location based service. [29]The identity can be a name, an ID, or any aggregation of the related key terms that is used to uniquely identify the user. [37]If a user makes its personal information showable to the location based services he/she can be badly hacked/attacked by an unauthorized persons who may be an attacker or adversary.

III. APPROACHES

For resolving Location Based Services (LBS) systems privacy issues to protect three attributes these are: Time, Identity & Location, a large amount of solutions are presented by different scientists recently and some of them are given below. But there are still some drawbacks in all approaches and it's still being explored by many scientists.

A. Path Confusion

[1]This method is about providing fake positions by hiding real location using anonymized pseudonyms, in this method user sends one or more fake location that is related to its real location but disadvantage is, if user is confusing path but still the user is sending information related to its nearby location that can be tracked. Algorithm for checking uncertainty of higher or lower privacy is:

$$H = -\sum pi \log pi$$

Where 'p' is probability of location and 'i' is target vehicle.

B. Silent Period

[1]In this method for a specific period of time system is put into a silent mode to avoid communication because of not being tracked by adversary after being free from this state location is updated to new one but disadvantage is, if vehicle's speed is below required then silent period will go long and location will not be updated and will remain old which is easy to track.

C. Swing And Swap

[1]In this approach a node can exchange its ID with nearest and parallel vehicle to confuse the attacker about vehicles but where user is on the less-populated road or on motorway then this technique is not efficient.

D. Cloud-Based Approach

[2]This approach defines that there are three main entities an LBS provider, a cloud server, and a group of LBS users. LBS provider registers a user on cloud server to authenticate the user. LBS user is provided with a secret key in order to prevent unauthorized access from individual user data in the whole cloud system. LBS user sends its personal information to service provider and service provider uploads its encrypted information to cloud server and cloud server responds to the query of user and after completing query to user cloud server expires the user and if user wants to reconnect to server then system revokes the user to the network. So by making a user registered with encryption key and after completing query making it expires establish a secure way of communication and protecting user privacy. But disadvantage of this technique is, most attackers know very well the decryption of encryption keys by applying most frequently used keys and also if nature of data is not very highly confidential and needs less encryption then we will waste our resources by applying heavy encryption algorithms which are expensive in implementation. And mismanagement of data size and required encryption algorithms should be managed according to the need of the current information.

E. Coordinate Transformation

In this technique user applies some [18] geometric operations like shifting and rotating over their locations before sending them to the LBS. In order to retrieve the original locations, inverses transformation function is used. This technique uses some mathematical operations like enlarging radius, shifting center, increasing the radius, or applying double obfuscation (i.e., mixing shifting center with any of remainders). But problem with this approach is that inverse transformation can be used to detect real information of the user.

F. Privacy-Supportive LBS Server

[3]In which server directly communicates with user. Server generates alerts about the privacy level of the user but it depends upon the user whether he/she will maintain these alerts or not. But disadvantage of this method is, user totally depends on server and if the server is out of order then it can generate wrong alerts to user which can misguide user about its privacy.

G. Cache-Based Approach

[3]In this method the data which is to be sent to server is saved in cache (a temporary memory) not permanently stored which is helpful to keep the attacker away from the data because data after using for a while is lost so that's why server does not grant access to any other entity. Main disadvantage is, this technique deals with cache not with server, which is not feasible when user generates query again to get the last-used data.

H. Optimal Mechanism

Which uses a [31] noise function which gives superlative compensation between privacy and profitability. In this approach method is generated through prompt methods like geometric, exponential, tight constraints that are efficient but there is no assurance of optimality. Generating the sound that causes disturbance via linear programming techniques, is computationally pricey, and not viable for more than about hundred locations, but it gives the most advantageous trade-off between privacy and efficacy.

I. Geo Indistinguishability

Which focuses on differential privacy which means to protect users information globally by some mathematical noise and [35] differential privacy aims to provide means to increases the accuracy of queries from statistical databases while decreases the chances of recognizing its audit and wrong information is passed to the system like if the user is in Paris but it will pose to be in London. But the problem is that user generates unneeded noise like if he is at the lake then it's useless to create noise.

J. Blind Filtering

[7]It includes semi trusted party, which is called proxy, for the filtering of our extra PIO (point of interest) records in a blind way. Semi server is not fully trusted that's why user is always ready to face an adverse condition It involves a semi trusted server that's why we have to rely on it. If service provider acts as user then semi-trusted server will send information to it rather than real user.

K. The L4NE Protocol

[5]It is a security protocol which addresses the privacy issues of LBS in equality testing by providing adequate security and performance and it is based on a composition of functions. In this protocol, we used n-self composition of functions. Self-composition functions are as secure as the discrete logarithm problem if a nonlinear function is selected properly. This is the proof that the L4NE protocol is as secure as most of the previously designed protocols if not more secure then some. Calculation of self-compositions is much faster than power functions. The L4NE protocol does not leak information of user to anyone. The L4NE protocol uses the commutative property of the composite function. But disadvantage of this technique is, if the nodes who are communicating with each other are found to be at the same exact location then it will reveal their information.

L. Homomorphism

[14]Which purpose is to maintain a surety level that centroid has been acquired without knowing the exact position of the user. [30]Afterwards a scheme public key privacy homomorphism is devised to accomplish location privacy. This is a TTP-free approach [30] which encrypts location of user by using a public key and LBS works to decrypt the information and share the results with all users who participated to compute centroid. But main issue with this method is decryption of location which can be used by malicious entity to cause attacks.

M. Geo indistinguishability by adding Laplace noise

[14]This technique protects user location privacy by producing continuous noise without any long pause at its coordinates by reducing personal identifiable information without affecting system's functionality. Disadvantage of this technique is that it just provides privacy regarding user's location which may be unnecessary for those who come with a different privacy requirement and also it's expensive.

N. Microaggregation-Based Approach

[14]The major standard of this methodology is to find out the centroid of at least K perturbed user locations by including zero-mean Gaussian noise and send directly to the LBS database server. [19]This method uses zero-mean which indicates that location is hard to find because there is no approximation of because of mean being zero and also Gaussian noise which is produced by poor illumination and high temperature or transmission independently. But main issue with this technique is: if user is static (staying at same location for a long time) then [30] the Gaussian noise can be repeatedly implemented to acquire the real location of the user.

O. Spatial Bloom Filtering

[23]It is used to determine the location and temporal information of the user. It uses a protocol which is based on direct communication of user and service provider where both entities are mutually distrusting each other, that's why they both don't want to disclose the private information to any third party. Where LBS only know the Area of Interest (AOI) of the user without knowing the exact location. Only generic area of the user is determined. Disadvantages of the proposed approach are following: [33]the relative location is only exposed when the user is within determined areas, [20]the provider estimates the distance from the central area to a certain extent, but the direction from which the user accesses stays private. Dividing the area around the point of interest in a different manner may disclose instead the direction but conceal the distance within the area range.

P. Content Cealed Bottle

[17] Content sealed bottle contains three main stages which are as follows: (1) Euclidean Distance Computation (2) A secure matching stage (3) A private POI retrieval stage. User generates a query attribute vector which is compared with the already saved vectors in the database server and Euclidean distance computation protocol finds

out the difference between both parameters. Secure matching stage is meant to search for the right match of attribute vector related to query of user. A technique the Garbled Circuit with optimized circuit modules for this phase to ominously condense the cost of whole construction of circuits. In the third step, a quadratic residuosity assumption (QRA) based private information retrieval protocol privately fetch the required point of interests for user. In this model server and clients are semi-honest, it means both follow the defined protocols but still they are curious to know each other. Moreover in this model, it is ensured that only user knows the final result of the query, while on the other hand, server's duty is responsible for the provision of relevant results and following the protocols. Basically Server hides its database and user hides its query. However, as the query is encrypted so server does not know about its content and user is concerned with accurate results. Disadvantages are listed as: A curious server/adversary can find out the actual content of query.

Q. Private Information Retrievel

It provides location privacy. [28]Using PIR techniques is favorable, the proposed approach requires the LBS provider uses a protocol to interact with users in an effective way. It keeps away the defined method to execute in real environments, where LBS provider is just interested in answering query of a user generated by a place without having to concern about privacy. So if this disadvantage could be overcome with low consumption of resources then this approach can be a great work for the research community in future.

R. Persona Technique

In this method user can generate asymmetric key-pair and share the public key with other users whom sender wants to send information. [32]Others users can be given a specified relationship with the sender and sender him/herself defines the level of every friend. Users can create groups and can add other users to make participant of the group and also can protect user's information by encryption method. User can also define some privacy policies like sharing data with some specific friends. Some cryptographic techniques are used for encryption and specification of the groups. Users are advised to select relationship clearly without any ambiguity like friend, colleague and university fellow. Created groups don't affect other groups and all participants can use them for encryption not only for decryption but there are some drawbacks in implementation of persona which are, [24]LBS server decrypts all coordinates of the position that's very difficult for the LBS server to even work on the closest-position queries. Without encryption attacker can easily crack down the location privacy of user and as a result Persona would fail in preserving privacy measures for users. Fetched information can be misused to destruct a user through irrelevant ads and attacks.

S. Context-Aware Privacy Protection

[22]In this approach a ranking function is used to rank all the users according to their exact distance from location and most importantly a LBS query is considered as top-k query. When server receives query it processes it against a spatial database and sends reply back to user. Location perturbing element disturbs the query-based location and reorganizes data for retrieval of actual location. Anonymous routing element leathers user ID through relaying nodes routing. It's very economical but there is a problem with it that is QoS (Quality of Service) hasn't given as much attention in anonymous networks.

Table I. Comparitive analysis of NTTP Mechanisms for Privacy Protection in LBS Systems

Sr. No.	*Name*	*Description*	*Scenario*	*Features*	*Limitations*
1	Path Confusion	Providing fake positions by hiding real location using anonymized pseudonyms, in this method user sends one or more fake location that is related to its real location	During travelling & used by vehicles	Confusing attacker about location services of vehicle	If user is confusing path but still the user is sending information related to its nearby location that can be tracked
2	Silent Period	For a specific period of time system is put into a silent mode to avoid communication because of not being tracked by adversary after being free from this state location is updated to new one	Travelling and involvement of vehicle to hide its identity	During silent period there is no chance of attack because of no communication	If vehicle's speed is below required then silent period will go long and location will not be updated and will remain old which is easy to track
3	Swing & Swap	A node can exchange its ID with nearest and parallel vehicle to confuse the attacker about vehicles	Travelling and used by vehicles	Nearest vehicle's id is exchanged with current node but as the travelling proceed ID keeps changing with different vehicles, does not rely on a same vehicle	Where user is on the less-populated road or on motorway then this technique is not efficient.
4	Cloud Based Approach	An LBS provider, a cloud server, and a group of LBS users. LBS provider registers a user on cloud server to authenticate the user. LBS user is provided with a secret key in order to prevent unauthorized access from individual user data in the whole cloud system	Used in Cloud based applications (online)	While connecting to internet privacy is more concerned so this method protects user from being attacked online	Most attackers know very well the decryption of encryption keys by applying most frequently used keys and also if nature of data is not very highly confidential and needs less encryption then we will waste our resources
5	Coordinate Transformation	User apply some geometric operations like shifting and rotating over their locations before sending them to the LBS	Location	There is no fully or semi trusted device at all just uses some simple but effective operations	Inverse transformation can be used to detect real information of the user.

6	Privacy Supportive LBS Server	Server directly communicates With user. Server generates alerts about the privacy level of the user but it depends upon the user whether he will maintain these alerts.	Web Services	Produces real time notifications when user's privacy is threatened	User totally depends on Server and if the server is out of order then it can generate wrong alerts to user which can misguide user about its privacy
7	Cache Based Approach	The data which is to be sent to server is saved in cache (a temporary memory) not permanently stored.	Mobile and any computing device	In case of very critical information attacker has less time to intrude because of cache.	This technique deals with cache not with server, which is not feasible when user generates query again to get the last-used data
8	Optimal Mechanism	Uses a [31]noise function which gives optimal trade-off between privacy and utility. In this approach method is generated through immediate method like geometric, exponential, tight constraints	Mechanism used during communication	It produces noise which is hard for attacker to know the right information due to its ambiguity.	Generating the noise via linear programming techniques, on the other hand, is computationally expensive, and not feasible for more than about hundred locations
9	Geo Indistinguishability	Focuses on [38]differential privacy which means to protect users' information globally by some mathematical noise and varying privacy targets to provide means to maximize the accuracy of queries from statistical databases.	Global level systems	Query based noise which hides the accuracy of query generated by database.	User generates unneeded noise like if he is at the lake then it's useless to create noise.
10	Blind Filtering	It includes semi trusted party, which is called proxy, for the filtering of our extra PIO (point of interest) records in a blind way.	Query-based privacy systems	Semi server is not fully trusted that's why user is always ready to face an adverse condition	It involves a semi trusted server that's why we have to rely on it. If service provider acts as user then semi-trusted server will send information to it rather than real user
11	L4NE Protocol	Security protocol which addresses the privacy issues of LBS in equality testing by providing adequate security and performance and it is based on a composition of functions.	Protocol used in networks for securing privacy	Composition functions are hard to decompose because of their length to nth value	If the nodes who are communicating with each other are found to be at the same exact location then it will reveal their information.
12	Homomorphism	[30]Ensure that centroid is calculated without any knowledge of the real location of the user. Later the identical concept of public key privacy homomorphism is proposed to attain privacy.	Location Based information	Both service provider and user don't trust each other and try to keep minimum information of each other	[30]Location decryption by LBS, makes this scheme susceptible and vulnerable to attacks.
13	Geo indistinguishability by adding Laplace noise	This technique protects user location privacy by producing continuous noise without any long pause at its coordinates by reducing personal identifiable information without affecting system's functionality.	Global Level Systems	Due to continuous noise there is no chance for an attacker to intervene	It just provides privacy regarding user's location which may be unnecessary for those who come with a different privacy requirement and also it's expensive
14	Micro-aggregation based scheme	Figure out the [19]centroid of at least K perturbed user locations by including zero-mean Gaussian noise and send directly to the LBS database server	Location based but involving vertices	Zero-mean because if average is known it's easy to track but with zero value it's difficult to track	If user is static (staying at same location for a long time) then [30]the Gaussian noise can be repeatedly implemented to acquire the original location of the user
15	Spatial Bloom Filter	Determine the location and temporal information of the user. It uses a protocol which is based on direct communication of user and service provider where both entities are mutually distrusting	Protocol targeting location and time	Both service provider and user don't trust each other and try to keep minimum information of each other	The [33]relative location is only disclosed when the user is within predetermined areas, the provider knows the distance from the central area to a particular criteria
16	Content concealed bottle	Achieve worthwhile query privacy preservation without the indulging of a third party or sacrificing the accuracy of LBSs	Query based protocol for communication	Each query sent over to the SP (service provider) is concealed in an efficient way	A curious server can search the real attributes in the query content sent by the user. Also can disturb the attributes similar to the real attributes in the user's query content.
17	PIR Approach	[28]It needs the LBS provider to co-operate with users by following the PIR protocol.	Retrieving information from database	Provide protocols/rules through which user can privately access its personal information stored anywhere	[28]It's hard to implement in real environment, where LBS providers just answer queries containing a location without any concern for location privacy
18	Persona	User generates an asymmetric key-pair and spread out the public key out-of-band to other users with whom they want to share data	Social Networking	It depends upon the will of user to customize accordingly only selected people are allowed to join the network	LBSAs directly would encrypt all location coordinates, making LBSAs incapable to progression nearest-neighbor queries. But if location is not encrypted, adversary using

					anonymized GPS traces success fully
19	Context-Aware Privacy Protection (CAP)	The LBS query is a top-k query with ranking function listed as the distance to the user's current location. After receiving the LBS query, the server runs it against a spatial database and sends result back to user.	Google Maps, data & network Communication	[22]The position perturbing component upsets the user's location. The anonymous routing component hides the user's network identity by routing the LBS query	QoS (Quality of Service) is lacking in CAP technique.

Sample of a Table footnote. (Table footnote)

IV. DISSCUSION AND RECOMMENDATIONS

The basic purpose is to protect user's privacy regarding time, position & identity. Above mentioned approaches protect some user's privacy attributes for provision of privacy. Now we elaborate all approaches according to some specific attributes given by them. Path Confusion only protects user location where vehicle is travelling, Silent Period also provides location privacy by updating the spatial information of the user, and Coordinate Transformation provides Location privacy by rotating and shifting the position. Swing & Swap protects User Identity by exchanging a vehicle's ID with nearest one. Cloud-Based approach also provides Identity protection by authentication of user in Cloud services. Privacy-Supportive LBS protects temporal information of user by generating alerts in web services. Cache Based approach provides Location & Identity privacy by querying the database server within specific timespan on mobile applications. Optimal Mechanism aims to protect spatial information by using noise function during communication. Geo Indistinguishability protects Location and Identity of user by mathematical noise in Global level services. Bloom Filtering just protects User Identity by adding a semi-trusted server in Query-Based privacy system. L4NE protocol protects only spatial information of user by using composite function in networks. Homomorphism only serves to protect User Identity & Location by computing centroid in Location Based Information. Geo Indistinguishability by adding Laplace Noise uses continuous noise function in protecting spatial information in Global level systems. Micro-aggregation protects Temporal & Spatial information by finding out centroid at the required time and hiding location by zero mean. Spatial Bloom Filtering protects Time and Identity of the user by a protocol. Content-Concealed Bottle protects Location and Identity of user by query privacy provision in query-based systems. Private Information Retrieval (PIR) protects only Identity of user by retrieving information from database. Persona only protects Location by protecting the user on social networking sites. And Context-Aware Privacy only deals to protect Location using ranking function in Google Maps & networks.

Although all these approaches served a great deal for preserving users' privacy but still these approaches do not cover all required attributes (Identity, Position & Time). All above techniques provide user with privacy but not with a complete level of satisfaction so there is always a chance for these techniques to break user's privacy, so we recommend to conduct a future work for the provision of such an NTTP approach which covers all three attributes to meet the requirement of user privacy goals. Giving user a free hand to find out their wanted locations without any fear of being intervened.

V. CONCLUSION

This survey paper firstly addressed the scope and worldwide usage of Location-Based Services (LBS) and limitations related to privacy in LBS, presented two ways of privacy preserving which are Non-Trusted Third Party (NTTP) and Trusted Third Party (TTP). Afterwards, marked some drawbacks in TTP related to reliance on third party, enhancing chances for privacy attacks. Indicates the significance of NTTP as compared to TTP where no trusted party is involved but the involvement of Non-Trusted Party is assured which reduces chances of privacy leakage. Later, Some NTTP approaches proposed with their features, description and disadvantages and compared all these approaches with each other to check out what privacy level these are serving to the users. We suggested some recommendations which are, provision of privacy for three attributes (User Identity, Time & Location) because missing even one attribute of them can lead to inadequate privacy provision which is a great threat for users. Moreover, handling to utilize resources efficiently to achieve these privacy attributes.

VI. ACKNOWLEDGMENT

This work was performed under auspices of Department of Computer Science and Information Technology, Govt. College Women University, Sialkot, Pakistan by Heir Lab-78. The Authors would like to thank Dr. M. Usman Ashraf for his insightful, and constructive suggestions throughout the research.

VII. REFERENCES

[1] Tyagi, Amit & Sreenath, N. (2015). A Comparative Study on Privacy Preserving Techniques for Location Based Services. British Journal of Mathematics & Computer Science. 10. 1-25.

[2] Lu Ou, Hui Yin, Zheng Qin, Sheng Xiao, Guangyi Yang, and Yupeng Hu, "An Efficient and Privacy-Preserving Multiuser Cloud-Based LBS Query Scheme," Security and Communication Networks, vol. 2018. 11 pages, 2018. https://doi.org/10.1155/2018/4724815.

[3] Alrahhal, Mohamad Shady & Khemakhem, Maher & Jambi, Kamal. (2017). A survey on privacy of location-based services: Classification, inference attacks, and challenges. Journal of Theoretical and Applied Information Technology. 3195.

[4] Konstantinos Chatzikokolakis, Ehab Elsalamouny, Catuscia Palamidessi, Anna Pazii. Methods for Location Privacy: A comparative overview. Foundations and Trends in Privacy and Security , Now publishers inc, 2017, 1 (4), pp.199-257.

[5] L Ertaul, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.3, March 2017

[6] Beye, M., Jeckmans, A., Erkin, Z., Erkin, Z., Hartel, P. H., Lagendijk, R., & Tang, Q. (2010). Literature Overview – Privacy in Online Social Networks. (CTIT Technical Report Series; No. TR-CTIT-10-36). Enschede: Centre for Telematics and Information Technology (CTIT).

[7] J. Chen, K. He, Q. Yuan, M. Chen, R. Du and Y. Xiang, "Blind Filtering at Third Parties: An Efficient Privacy-Preserving Framework for Location-Based Services," in *IEEE Transactions on Mobile Computing*.

[8] Jinxing Qu, Guoyin Zhang, and Zhou Fang, "Prophet: A Context-Aware Location Privacy-Preserving Scheme in Location Sharing Service," Discrete Dynamics in Nature and Society, vol. 2017, Article ID 6814832, 11 pages, 2017.

[9] Li Kuang, Yin Wang, Pengju Ma, et al., "An Improved Privacy- Preserving Framework for Location-Based Services Based on Double Cloaking Regions with Supplementary Information Constraints," Security and Communication Networks, vol.2017, Article ID 7495974, 15 pages, 2017.

[10] Chen, L , Thombre , S , Järvinen , K , Lohan , E S , Alén-Savikko , A , Leppäkoski , H , Bhuiyan , M Z H , Bu-Pasha , S , Ferrara , G N , Honkala , S , Lindqvist , J , Ruotsalainen , L , Korpisaari , P & Kuusniemi , H 2017, ' Robustness, Security and Privacy in Location-Based Services for Future IoT : A Survey ' IEEE Access , vol. 5, pp. 8956-8977.

[11] Mohammad Yamin, Adnan Ahmed Abi Sen, "Improving Privacy and Security of User Data in Location Based Services", International Journal of Ambient Computing and Intelligence, 2018

[12] Anuar, Faiz & Gretzel, Ulrike. (2011). Privacy Concerns in the Context of Location-Based Services for Tourism.

[13] Aloudat, Anas & Michael, Katina & Yan, J. (2018). Location-Based Services in Emergency Management-from Government to Citizens: Global Case Studies. Faculty of Informatics – Papers.

[14] Ruchika Gupta and Udai Pratap Rao, "A Hybrid Location Privacy Solution for Mobile LBS," Mobile Information Systems, vol. 2017, Article ID 2189646,11 pages, 2017.

[15] Palmieri P., Calderoni L., Maio D. (2015) Spatial Bloom Filters: Enabling Privacy in Location-Aware Applications. In: Lin D., Yung M., Zhou J. (eds) Information Security and Cryptology. Inscrypt 2014. Lecture Notes in Computer Science, vol 8957. Springer, Cham.

[16] Solanas, Agusti & Domingo-Ferrer, Josep & Ballesté, Antoni. (2008). Location Privacy in Location-Based Services: Beyond TTP-based Schemes. CEUR Workshop Proceedings. 397.

[17] Qin Hu Shengling Wang, Chungiang Hu, Jianhui Huang, Wei Li, Xiuzhen Cheng, "Messages in a Concealed Bottle: Achieving Query Content Privacy with Accurate Location-Based Services", IEEE Transactions on Vehicular Technology, 2018

[18] Wernke, Marius, Pavel Skvortsov, Frank Dürr, and Kurt Rothermel. "A classification of location privacy attacks and approaches", Personal and Ubiquitous Computing, 2014.

[19] "Achieving location privacy through CAST in location based services", Journal of Communications and Networks, 2017

[20] "Spatial Bloom Filters: Enabling Privacy in Location Aware Applications", Lecture Notes in Computer Science, 2015.

[21] Shabana Habib, Somaila Saleem, Khawaja Muhammad Saqib, "Review on MANET routing protocols and challenges", 2013 IEEE Student Conference on Research and Development, 2013

[22] Aniket Pingley, Wei Yu, Nan Zhang, Xinwen Fu, Wei Zhao "A context-aware scheme for privacy-preserving location-based services", Computer Networks, 2012

[23] Piao, Chunhui, Xiaoyan Li, Xiao Pan, and Changyou Zhang, "User privacy protection for a mobile commerce alliance", Electronic Commerce Research and Applications, 2016.

[24] Puttaswamy, Krishna P. N., Shivuan Wang, Troy Steinbauer, Divyakant Agrawal, Amr El Abbadi, Christopher Kruegel, and Ben Y. Zhao, "Preserving Location Privacy in Geo-Social Applications", IEEE Transactions on Mobile Computing, 2012.

[25] Vincent Primault, Antoine Boutet, Sonia Ben Mokhtar, Lionel Brunie, "The Long Road to Computational Location Privacy: A Survey", IEEE Communications Surveys & Tutorials, 2018

[26] Ruchika Gupta, Udai Pratap Rao, "An Exploration to Location Based Service and Its Privacy Preserving Techniques: A Survey", Wireless Personal Communications, 2017

[27] "University of Macau | The only public comprehensive university in Macau", Um.edu.mo, 2018. [Online]. Available: http://www.um.edu.mo/. [Accessed:17-Dec-2018].

[28] "CRISES/URV", *Crises-deim.urv.cat*, 2018. [Online]. Available: https://crises-deim.urv.cat/web/. [Accssesd: 17-Dec-2018].

[29] "OPUS: Zur Startseite", *Elib.uni-stuttgart.de*, 2018. [Online]. Available: https://elib.umi-stuttgart.de/. [Accessed: 17-Dec 2018].

[30] "Home – Springer", *Link.springer.com*, 2018. [Online]. Available: https://link.springer.com/. [Accessed: 17-Dec-2018].

[31] "Inria – Accueil", *Hal.inria.fr*, 2018. [Online]. Available: https://hal.inria.fr/. [Accessed: 17-Dec-2018].

[32] "Computer Communication Review | acm sigcomm", Sigcomm.org, 2018. [Online]. Available: http://www.sigcomm.org/publications/computer-communication-review. [Accessed: 17-Dec-2018].

[33] "CORA Home", *Cora.ucc.ie*, 2018. [Online]. Available: https://cora.ucc.ie/. [Accessed: 17- Dec- 2018].

[34] "INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES", *Ijcsit.com*, 2018. [Online]. Available: 2018].

[35] 2018. [Online]. Available: https://downloads.cloudsecurityalliance.org/. [Accessed: 17-Dec-2018].

[36] "PoPETs/PETS", *Petsymposium.org*, 2018. [Online]. Available: https:// petsymposium.org/. [Accessed: 17-Dec- 2018].

[37] "IJARCCE - A Monthly Peer-reviewed Online Journals", *IJARCCE*, 2018. [Online]. Available: https:// ijarcce.com/. [Accessed: 17-Dec-2018].

[38] "CryptoWiki", *Cryptowiki.net*, 2018. [Online]. Available: http://cryptowiki.net/index.php?title=Main_Page. [Accessed: 17-Dec-2018].