ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Certain Investigations on Securing Moving Data Objects

P.Andrew[1], J.Anish Kumar[2], R.Santhya[3], Prof.S.Balamurugan[4], S.Charanyaa[5]

Department of IT, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1,2,3,4]

Senior Software Engineer Mainframe Technologies Former, Larsen & Tubro (L&T) Infotech, Chennai TamilNadu, India[5]

ABSTRACT: Recently there is a steep rise in usage of location –aware devices such as many GSM mobile phones, GPS enabled PDA's, location sensors, and active RFID tags. Due to this device usage scenario, the device generate a large collection of moving data objects with the help of trajectory data , all these data are used for various data identification and analysis process. For instance consider traffic control, one can hack the control unit of traffic control management. Therefore it is way clear that a hacker may collect many temporal data to cover sensational massages of an organization and especially he/she can discover much personal information of third party/check points of many premises. Typically personal data (data privacy) may also fetch. Due to user's identity replacement which is actual like terminal i.e. Quasi Identifiers (QID) of moving data are linked to external information to re-identify individual existence, thus the attacker can be able to track and trace the anonymous moving objects back into individuals. This paper gives a survey on recent trends and a new strategy for securing trajectory moving data objects.

KEYWORDS: GSM, Trajectory Data, Moving Object Data, Data Privacy, Quasi Identifier, Security Attack.

I. Introduction

Several authors have undergone many survey and created their algorithms in securing moving object data. The main objective is that is to hide the spatio-temporal data to the anonymous user. The major reason is that to protect the isolated data. Since data privacy preserving is been our major goal we can do various research in this field. Ghinita et al. [44][2009] considered two conceal mechanisms in which an adversary background knowledge of maximum speed to infer more specific location information. Based on the velocity of the movement of the object the attacker could assume that the object is under a particular movement as an example if Alice is walking on the road based on her velocity of speed the attacker could find that Alice is waling if she is driving a car the attacker could find that she is driving. So based on the velocity based adversary knowledge the trajectory data could be predicted. So Ghinita considered two types of attacks: (1) the initiative without back ground information more on sensitive location map. (2) The initiative with such background information. In the first case, the privacy requirement is not allow to an attacker to diagnose the user location in the sub-region in the pretext region. In the second case, the privacy requirement direct that the probability of association between the user and the location. She consider two types of transformation on trajectory databases, temporal and spatial cloaking. The author planned two alternatives in achieving temporal cloaking: request deferral and postdating. The space and time error are generated in the temporal cloaking and spatial cloaking. In this for the low velocity the request are safe but in the case that the velocity increases the request are deferred/postdated. As the velocity increases the request for temporal data should be processed while moving. Correlation-based adversary knowledge: In this data publishing most of the attacker uses this correlation-based adversary knowledge because the attacker attain by correlating the timestamps of the user. The attacker finds the highest probability of the user location by forward motion and the backward motion model during a period of time the attacker correlates the user location by their movement. Jin et al [45]. Implemented two protocols for publishing the data. In the first they cluster the location of the users and then the data is published if the forward breach probability is below the user-defined threshold. Then they re-cluster the data at a period of time and find out the backward breach probability, by correlating forward breach probability and backward breach probability the data is published if the data does not reach the user-defined threshold. But these approaches are more effective to defend against the attacks but not to stop it.

Even though the location privacy has already been accepted as an important problem and effective privacy-preserving solutions to publish the trajectories data. These trajectories data might be defined by user itself and by data mining the databases. In this world's technology for positioning systems, the location of the trajectories data can be predicted very accurately. The location data can be obtaining through the score pairs i.e. longitude and latitude. The location can also be finding out by QIDs by identifying the frequent mining pattern technique. The QID mining looks for the frequently mined pattern and correlated with the threshold defined by the user.

The remainder of the paper is organized as follows. Section 2 deals about Literary Review and Recent Trends. Objectives are designed and are discussed in Section 3. Section 4 portrays the Working Methodology. Section 5 concludes the paper and outlines the direction for Future Work

II. Literary Review And Recent Trends

In 2009b [27] authors said that nowadays the wireless networks are improving the widespread and also the lacking of technique for locating a device has also been increased efficiently. There are some techniques for verifying and guarantying a location given by the user without dome specialized software particularly in large scale networks through the Location Based Services (LBS). Usually in some of the application a device is in need o authenticate by itself to other in some way which usually takes the form of interchanging a private secret share by two like password, in order to prove the identity of the device. While the device to produce the password which disclose the password and allow the access, it is enough for the device to prove its current location is in the area of that network. This kind of location verification problems can be resolved by the methods like Active Badge and RFID. The major limitation of this method is that these are relay within a constrained area and also need an infrastructure of sensors to perform some function which inturn aims its usage to small scale network. For large scale, Vehicular Adhoc Networks (VANETs) is used which does not require any special physical infrastructure. This scheme is been chosen because of the protocol's requirements of lameper-resistent devices and also the public key cryptography.

In 2009 c [28] this paper, the author presented results of a large-scale quantitative analysis of Brightkite, a commercial location-based social network (LSN). Unlike other social networks, Brightkite is dominated by male users who are professionals and likely to be bloggers and work in social media area. High-degree users are likely more mobile, have more friends, and send more updates. SMS and Email users are more mobile and their location updates are harder to predict. By clustering the attributes from profiles, activities, mobility, and social graphs, we can classify all users into five distinct behaviour groups. In future work, the author plan to expand their future work on the studies of social graphs using additional metrics and combine them for correlated analysis. The author also plans to extract a workload model from the location updates to evaluate the performance of location based information-sharing and privacy-preserving algorithms.

In 2010b [30] the author made a survey of recent advancements for the offering of K–anonymity in LBSs. Most of the approaches that have been proposed heavily depend on a trusted server component – that acts as an intermediate between the end user and the service provider – to preserve the anonymity of the former entity. Existing approaches are partitioned in three categories: (a) historical K–anonymity, (b) location K–anonymity, and (c) trajectory K–anonymity. In each of these categories we present some of the most prevalent methodologies that have been proposed and highlight their operation. The author informed us that the future work in this research direction will lead to more robust and thorough methodologies that better protect the privacy of the user when requesting LBSs. In 2010c [31], the author showed that their methods yield a formal theoretical protection guarantee against the re-identification attack. Through an extensive set of experiments on a real-life spatio-temporal dataset and showed that the anonymity protection achieved is considerably stronger than the theoretical worst case and the proposed techniques preserve the quality of the clustering analysis. The whole anonymization process is based on different steps using different transformation tools. At the moment there is no a strict integration of consecutive steps, although it is believed that there several margins to improve the quality of the anonymization. The author also suggested as that the further investigations could be directed to developing a generalization method that considers both spatial and temporal information in order to obtain generalized and anonymous spatio-temporal data.

In 2011b [33] the author presented decentralized methods that accomplish the efficiency of mobile devices to make wireless personal ad-hoc networks to preserve the security of users who can approach location-based services. The uniqueness of this approach is that users do not need to trust any party such as an intermediary server or peers with their locations and identities. The author also proposed an efficient algorithm for users to estimate a k-anonymous imprecise location and to randomly choose one of her peers with uniform probability who forwards the service request on behalf of the user. The author also shows an experimental evaluation using this approach can enjoy a high quality of service with a high degree of privacy.

In 2011c [34]author spoke about the extension of mobile devices with global positioning functionality like GPS and AGPS and Internet connectivity such as 3G and Wi-Fi has resulted in widespread development of location-based services (LBS). For snapshot LBS, a mobile user only needs to report its current location to a service provider once to get its desired information. On the other hand, a mobile user has to report its location to a service provider in a periodic or on-demand manner to obtain its desired continuous LBS. Protecting user location privacy for continuous LBS is more challenging than snapshot LBS because intruders may use the spatial and temporal correlations in the user's location samples to infer the user's location information with higher certainty. Such user location trajectories are also very important for many applications. However, publishing such location trajectories to the public or a third party for data analysis could have serious privacy concerns. Privacy protection in continuous LBS and trajectory data publication has increasingly drawn attention from the research community and industry.

In 2012b [35], the author stated the classification of L2P2 problems into Basic L2P2 and Enhanced L2P2 problems. The difference between basic and enhanced L2P2 lies in whether the common users or all users in a sequence of cloaking areas would be used for privacy computation. For basic L2P2, a design of simple algorithm cloaking Algorithm1 is designed to address this problem. While for enhanced L2P2, the author proposed four heuristics like Cloaking Algorithm 2 for Enhanced L2P2, Cloaking Algorithm 3 for Enhanced L2P2, Cloaking Algorithm 4 for Enhanced L2P2 and Cloaking Algorithm 3 for Enhanced L2P2 to generate cloaking areas to satisfy users' privacy requirements, where each heuristic has a different, unique criterion to expand cloaking areas. In addition, to evaluate the effectiveness of this proposed algorithms, they conducted a large number of simulations, and several interesting observations have been reported.

The author also forwarded the future work as follows,

1) Investigate other efficient heuristics for enhanced L2P2 problem.

2) Test the proposed methods over other location data sets and try different location privacy measurements.

In 2012c [36], the author stated that accessing location-based services from mobile devices entails a privacy risk for users whose sensitive information can be inferred from the locations they visit. This information leakage raises the need for robust location-privacy protecting mechanisms (LPPMs). This LPPM is designed to provide user-centric location privacy; hence it is ideal to be implemented in the users' mobile devices. This method accounts for the fact that the strongest adversary not only observes the perturbed location sent by the user but also knows the algorithm implemented by the protection mechanism. Hence, he can accomplish the information leaked by the LPPM's algorithm to minimize his uncertainty about the user's true location. However, the user is only aware of the adversary's knowledge and does not make any assumption about his inference attack. Hence, she prepares the protection mechanism against the most optimal attack. By modelling the problem as a Bayesian Stackelberg competition, the author ensures that the optimal LPPM is designed anticipating such strong inference attack and also validated their method using real location traces. They have demonstrated that their approach finds the optimal attack for a given LPPM and service-quality constraint, and also shown that it is superior to other LPPMs such as basic location obfuscation where the optimal LPPM over alternatives is more significant when the service-quality constraint imposed by the user is tightened. Hence, this solution is effective exactly where it will be used. Finally, the results confirmed that loosening the service-quality constraint allows for increased privacy protection, but the magnitude of this increase strongly depends on the user profile, i.e., on the degree to which a user's location is predictable from her LBS access profile. To the best of author's knowledge, this is the first framework that explicitly includes the adversarial knowledge into a privacy-preserving design process, and considers the common knowledge between the privacy protector and the attacker.

In 2013 b [39] authors showed the present utilization of uncertainty information in a selection of applications in a mobile and also show the possibility of introducing artificial uncertainty into location information while using LBS without illustrating it. In 2013 c [40], the author proposed a new technique called a novel tree-based divisionary routing principle for protecting source location privacy using hide and seek strategy. This will also minimize energy consumed in hotspot and produce redundancy tactic routes in the non hotspot regions with abundant energy. Hence it achieves the maximization of the network lifetime and not only the preservation of privacy of a data.

In 2014 b [42], the author proposed a concept of fine grained privacy preserving location based service (LBS) framework called FINE which is basically for mobile devices. Also the authors proposed FINE framework combines the transformation key and proxy re-encryption to more most of computation –intensive tasks from the LB's provides and also the cloud server or 3rd party uses which also keep the mobile devices for away from significant resource consuming operations. The further analysis of this FINE framework shows that it is source and highly efficient for mobile devices in the terms of communication and execution cost. The author laid the future work is that to reduce the cost on the cloud server lower the trust user on the cloud server honest but curious to introducers and also to calculates the effectiveness of the proposed FINE framework.

In 2014c [43], the author stated that the LBS have become an important part of our regular life. The untrusted LBS server will have information about the users in LBS and it will trace them in a different ways or also they can disclose their information to 3rd party which affects the person physically and mentally. Inorder to overcome this problem, the author suggested to use Dummy-Location Selection (DLS) algorithm which is been used inorder to attain k-anonymity for the users in LBS. The features of DLS are out of box from the existing approaches which keenly choose dummy location and also have a care about the protection of data from intruders. Firstly, on the entropy metric, the dummy locations are identified, then to assure that the selector dummy location are spread far as possible, the enhanced-DLS algorithm is been proposed. This algorithm can also enlarge the cloaking region (CR) by keeping same privacy level as the DLS algorithm.

III. Objectives

Even though privacy has been protected there are few open problems the two fundamental that are taken as objectives of our project:

1. Identifying secured moving data objects with high probability (Granularities of QID Location)

Though we trace people with help of modern technology such as GPS, mobile trackers, GIS, tracking IMEI number etc. we can be very accurately identify the spatial areas of the person or living area etc. There are several approaches to ascertain QID of various granularities. Ascertaining the granularity of QID location is an important and accosts problems. The locations of moving objects can be recorded precisely, down to the level of (Longitude, latitude) pairs. Kido et al divide the space into several regions. The bandit knowledge of position information of attacker is delimited by region which it belongs to. Monreale et al.[3][] consider the syntactic trajectory, which reasons over trajectories from a syntactic point of view define sensitive spatial areas and QID based on “privacy places” taxonomy. Finding the definition of quasi-identifiers in a pragmatic and triable and countable way is an open problem to hide the anonymity trajectory data in identifying the moving objects with high probability is an open problem.

2. Quick & Efficient discovery of QID of moving data objects:

Since many emerging trends assure that QID can provide either directly by end-user at the time he/she subscribe to location based service. In the QID aware anonymization technique the maximal size of the QID has a cogent collision on the algorithm performance. While run-time grows sub linearly with k, it grows super-linearly with the maximal size of the QIDs which make the performance of the algorithm less. In the case of anonymization, if the database is less, redundancy is less and location point is small, then the unification for the trajectories of moving objects is bungle. In the QID blind anonymization technique comparing with generalization approach and point matching the generalization-based technique the generalized locations are betrayed uncontrolled information about exact locations of the points and the generalized trajectories may become useless for data mining and statistical applications which work on diminutive trajectories. After reconstruction on data publishing rather than data anonymized by means of generalization. The reconstruction is atomic and suitable for trajectory data mining applications. According to Mohammed et al.[4][] he used two algorithm (1) Apriori algorithm (2) Greedy algorithm. In the Apriori algorithm the solution to find out to avoid enumerating all possible violating sequences the authors aims to find minimal violating sequences. The q set violates LKC-privacy requirement, which stores minimal, violates sequences, to generate the next candidate set which has non-violating sequence set. The Greedy Algorithm impute the initial Score (p) to every candidate pair. In each monotony, the highest score pair will be suppressed, the remaining score pair are updated until no candidate pair monotony is available. If data to be accessed so by suppressing the data will make data under-utilized.

IV. Proposed Methodology

For the intended use of data the adhoc anonymization technique is used for the location privacy data. Work in query evaluation over uncertain databases can hence be used for answering adhoc queries over anonymized data i.e. trajectory data.

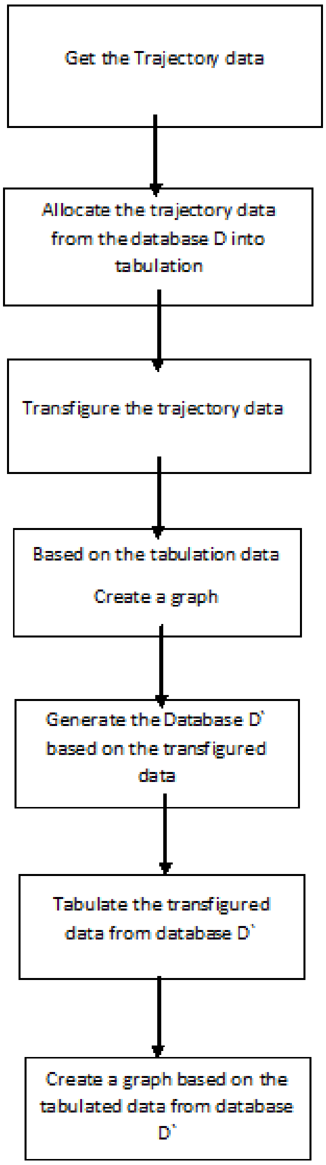
Get the Trajectory data
Allocate the trajectory data from the database D into tabulation
Transfigure the trajectory data
Based on the tabulation data Create a graph
Generate the Database D` based on the transfigured data
Tabulate the transfigured data from database D`
Create a graph based on the tabulated data from database D`

Fig 1 Workflow of the Proposed Methodology

V. Conclusion and Future Work

Allocating the trajectory data from the database D into a tabulation method and based on that tabulation creating a graph and transfiguring the trajectory data as database D` and tabulating it and creating the graph based point and apply the point of matching and publish the data. So the attacker will match the points in the graph and trying all the possibilities and also trying the trajectory data in the database D`. Typically personal data (data privacy) may also fetched. Due to user's identity replacement which is actual like terminal i.e. Quasi Identifiers (QID) of moving data are linked to external information to re-identify individual existence, thus the attacker can be able to track and trace the anonymous moving objects back into individuals. This paper rendered a survey on recent trends and a new strategy for securing moving data objects.

REFERENCES

1. Solomon, Toby. "Personal Privacy and the 1984 Syndrome." *W. New Eng. L. Rev.* 7: 753,1984
2. Cox, L. H., Bruce Johnson, Sarah-Kathryn McDonald, Dawn Nelson, and Violeta Vazquez. "Confidentiality issues at the Census Bureau." In *Proceedings of the First Annaul Census Bureau Research Conference, Washington, DC: US Government Printing Office*, pp. 199-218. 1985.
3. Duncan, George T., and Diane Lambert. "Disclosure-limited data dissemination." *Journal of the American statistical association* 81, no. 393: 10-18, 1986.
4. Simitis, Spiros. "Reviewing privacy in an information society." *University of Pennsylvania Law Review* : 707-746, 1987.
5. Melton, Gary B. "Must researchers share their data?." *Law and Human Behavior* 12, no. 2: 159, 1988.
6. Laster, Daniel. "Breaches of Confidence and of Privacy by Misuse of Personal Information." *Otago L. Rev.* 7 : 31, 1989.
7. Flaherty, David H. "On the utility of constitutional rights to privacy and data protection." *Case W. Res. L. Rev.* 41: 831, 1990.
8. Maciorowski, Linda F. "The enduring concerns of privacy and confidentiality."*Holistic nursing practice* 5, no. 3: 51-56, 1991.
9. Davies, Simon G. "Constructing an International Watchdog for Privacy and Data Protection: The Evolution of Privacy International." *JL & Inf. Sci.* 3: 241, 1992.
10. Regan, PriscllaM. "The Globalization of Privacy." *American Journal of Economics and Sociology* 52, no. 3: 257-274, 1993.
11. Johnson, Donald Byron, Stephen M. Matyas, An V. Le, and John D. Wilkins. "The commercial data masking facility (CDMF) data privacy algorithm." *IBM Journal of Research and Development* 38, no. 2: 217-226, 1994.
12. O'Leary, Daniel E., S. Bonorris, W. Klosgen, Yew-Tuan Khaw, Hing-Yan Lee, and W. Ziarko. "Some privacy issues in knowledge discovery: the OECD personal privacy guidelines." *IEEE Expert* 10, no. 2: 48-59, 1995.
13. Ferrer, Josep Domingo I. "A new privacy homomorphism and applications."*Information Processing Letters* 60, no. 5: 277-282, 1996.
14. Duncan, George T., and Stephen E. Fienberg. "Obtaining information while preserving privacy: A markov perturbation method for tabular data." In *Joint Statistical Meetings*, pp. 351-362. 1997.
15. Samarati, Pierangela, and Latanya Sweeney. *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression*. Technical report, SRI International, 1998.
16. Brankovic, Ljiljana, and Vladimir Estivill-Castro. "Privacy issues in knowledge discovery and data mining." In *Australian institute of computer ethics conference*, pp. 89-99. 1999.
17. Choy, Manhoi, Mei-Po Kwan, and Hong V. Leong. "Distributed database design for mobile geographical applications." *Journal of Database Management (JDM)*11, no. 1: 3-15, 2000.
18. Pfoser, Dieter, and Christian S. Jensen. "Querying the trajectories of on-line mobile objects." In *Proceedings of the 2nd ACM international workshop on Data engineering for wireless and mobile access*, pp. 66-73. ACM, 2001.
19. Trajcevski, Goce, Ouri Wolfson, Fengli Zhang, and Sam Chamberlain. "The geometry of uncertainty in moving objects databases." In *Advances in Database Technology—EDBT 2002*, pp. 233-250. Springer Berlin Heidelberg, 2002.
20. Ashbrook, Daniel, and Thad Starner. "Using GPS to learn significant locations and predict movement across multiple users." *Personal and Ubiquitous Computing* 7, no. 5: 275-286, 2003.
21. Gruteser, Marco, and Xuan Liu. "Protecting privacy in continuous location-tracking applications." *IEEE Security & Privacy* 2, no. 2 : 28-34, 2004.
22. Bettini, Claudio, X. Sean Wang, and Sushil Jajodia. "Protecting privacy against location-based personal identification." In *Secure Data Management*, pp. 185-199. Springer Berlin Heidelberg, 2005.
23. An, Xiangdong, Dawn Jutla, and Nick Cercone. "Dynamic inference control in privacy preference enforcement." In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, p. 24. ACM, 2006.
24. Lee, Jae-Gil, Jiawei Han, and Kyu-Young Whang. "Trajectory clustering: a partition-and-group framework." In *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, pp. 593-604. ACM, 2007.
25. Abul, Osman, Francesco Bonchi, and Mirco Nanni. "Never walk alone: Uncertainty for anonymity in moving objects databases." In *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, pp. 376-385. Ieee, 2008.
26. Bonchi, Francesco. "Privacy preserving publication of moving object data." In*Privacy in Location-Based Applications*, pp. 190-215. Springer Berlin Heidelberg, 2009.
27. Graham, Michelle, and David Gray. "Protecting Privacy and Securing the Gathering of Location Proofs–The Secure Location Verification Proof Gathering Protocol." In *Security and Privacy in Mobile Information and Communication Systems*, pp. 160-171. Springer Berlin Heidelberg, 2009.
28. Li, Nan, and Guanling Chen. "Analysis of a location-based social network." In*Computational Science and Engineering, 2009. CSE'09. International Conference on*, vol. 4, pp. 263-270. IEEE, 2009.
29. Shokri, Reza, Julien Freudiger, and Jean-Pierre Hubaux. *A unified framework for location privacy*. No. EPFL-REPORT-148708. 2010.
30. Gkoulalas-Divanis, Aris, Panos Kalnis, and Vassilios S. Verykios. "Providing k-anonymity in location based services." *ACM SIGKDD Explorations Newsletter*12, no. 1 (2010): 3-10.
31. Monreale, Anna, Gennady L. Andrienko, Natalia V. Andrienko, Fosca Giannotti, Dino Pedreschi, Salvatore Rinzivillo, and Stefan Wrobel. "Movement Data Anonymity through Generalization." *Transactions on Data Privacy* 3, no. 2 (2010): 91-121.
32. Chow, Chi-Yin, and Mohamed F. Mokbel. "Trajectory privacy in location-based services and data publication." *ACM SIGKDD Explorations Newsletter* 13, no. 1 (2011): 19-29.
33. Hashem, Tanzima, and Lars Kulik. ""Don't trust anyone": Privacy protection for location-based services." *Pervasive and Mobile Computing* 7, no. 1 (2011): 44-59.
34. Bonchi, Francesco, Laks VS Lakshmanan, and Hui Wendy Wang. "Trajectory anonymity in publishing personal mobility data." *ACM Sigkdd Explorations Newsletter* 13, no. 1 (2011): 30-42.

35. Pan, Xiao, Jianliang Xu, and Xiaofeng Meng. "Protecting location privacy against location-dependent attacks in mobile services." *Knowledge and Data Engineering, IEEE Transactions on* 24, no. 8 (2012): 1506-1519.

36. Wang, Yu, Dingbang Xu, Xiao He, Chao Zhang, Fan Li, and Bin Xu. "L2P2: Location-aware location privacy protection for location-based services." In*INFOCOM, 2012 Proceedings IEEE*, pp. 1996-2004. IEEE, 2012.

37. Shokri, Reza, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. "Protecting location privacy: optimal strategy against localization attacks." In *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 617-627. ACM, 2012.

38. Miura, Kenta, and Fumiaki Sato. "A Hybrid Method of User Privacy Protection for Location Based Services." In *Complex, Intelligent, and Software Intensive Systems (CISIS), 2013 Seventh International Conference on*, pp. 434-439. IEEE, 2013.

39. Merrill, Shawn, Nilgun Basalp, Joachim Biskup, Erik Buchmann, Chris Clifton, Bart Kuijpers, Walied Othman, and Erkay Savas. "Privacy through uncertainty in location-based services." In *Mobile Data Management (MDM), 2013 IEEE 14th International Conference on*, vol. 2, pp. 67-72. IEEE, 2013.

40. Long, J., M. I. A. N. X. I. O. N. G. Dong, K. A. O. R. U. Ota, and A. N. F. E. N. G. Liu. "Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks."*Access, IEEE* 2 (2014): 633-651.

41. Wernke, Marius, Pavel Skvortsov, Frank Dürr, and Kurt Rothermel. "A classification of location privacy attacks and approaches." *Personal and ubiquitous computing* 18, no. 1 (2014): 163-175.

42. Shao, Jun, Rongxing Lu, and Xiaodong Lin. "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices." In *INFOCOM, 2014 Proceedings IEEE*, pp. 244-252. IEEE, 2014.

43. Niu, Ben, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. "Achieving k-anonymity in privacy-aware location-based services." In *Proc. IEEE INFOCOM*. 2014.

44. Ghinta, G, Damiani, M. L., Silverstri, C.,and Bertino, E. Preventing velocity linkage attacks in location –aware applications. In Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (2009), pp.246-255.

45. Jin, W., Lefevre, k, and Patel, J. M. An online framework for publishing privacy-sensitive location traces. In Proceedings of the Ninth ACM International Workshop on Data engineering for wireless and Mobile Access (2010).

46. Monreale, A., Trasart, R., Renso, C., Pedreschi, D., and Bogorny, V. Preserving privacy in semantic-rich trajectories of human mobility. In Proceedings of the 3rd ACM SIGSPAIAL International workshop on security and Privacy in GIS and LBS (2010), pp. 47-54.

47. Mohammed, N., FungG, B. C., and Debbabi, M. Walking in the crowd: anonymzing trajectory data for pattern analysis. In Proceeding of the 18th ACM conference on Information and knowledge management (2009), pp. 1441-1444.

BIOGRAPHY

P.Andrew J.Aneesh and R.Santhya are currently pursuing their B.Tech. degree in Information Technology at KalaignarKarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India. Their areas of research interests include Network Security, Cloud Computing and Database Security.

Prof.S.Balamurugan obtained his B.Tech degree in Information Technology from P.S.G. College of Technology, Coimbatore, Tamil Nadu, India and M.Tech degree in Information Technology from Anna University, Tamil Nadu, India respectively. He is currently working towards his PhD degree in Information Technology at P.S.G. College of Technology, Tamil Nadu, India. At present he holds to his credit **50 papers International Journals and IEEE/ Elsevier International Conferences.** He is currently working as Assistant Professor in the Department of Information Technology, Kalaignar Karunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India affiliated to Anna University TamilNadu, India. He is **State Rank holder** in schooling. He was **University First Rank holder** M.Tech. Semester Examinations at Anna University, Tamilnadu, India. He served as a Joint Secretary of IT Association, Department of Information Technology, PSG College of Technology, Coimbatore, Tamilnadu, India. He is the **recipient of gold medal and certificate of merit** for best journal publication by his host institution **consecutively for 3 years**. Some of his professional activities include invited Session Chair Person for two Conferences. He has guided 12 B.Tech projects and 2 M.Tech. projects. He has won a best paper award in International Conference. His areas of research interest accumulate in the areas of Data Privacy, Database Security, Object Modeling Techniques, and Cloud Computing. He is a life member of ISTE,CSI. **He has authored a chapter in an International Book "Information Processing" published by I.K. International Publishing House Pvt. Ltd, New Delhi, India, 978-81-906942-4-7. He is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**

S.Charanyaa obtained her **B.Tech** degree in Information Technology and her **M.Tech** degree in Information Technology from Anna University Chennai, Tamil Nadu, India. She was **gold medalist** in her B.Tech. degree program. She has to her credit **12 publications in various International Journals and Conferences**. Some of her outstanding achievements at school level include **School First Rank holder** in **10th and 12th grade**. She was working as Software Engineer at Larsen & Turbo Infotech, Chennai for 3 years where she got promoted as Senior Software Engineer and worked for another 2 years. She worked at different verticals and worked at many places including Denmark, Amsderdam handling versatile clients. She is also the recipient of **best team player award for the year 2012 by L&T**. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Cloud Computing. **She is the author of book titled "Principles of Social Network Data Security", ISBN: 978-3-659-61207-7.**