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

Investigations on Evolution of Strategies to Preserve Privacy of 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: This paper reviews methods to protect moving data objects for the past 30 years. Data Disclosure Preventing Techniques such as disclosure limiting and ad-hoc approval publishing data are depicted. Privacy Homomorphism And Encryption Methods such as Data Protection Directive, Commercial Masking facility algorithm, Data Encryption Algorithm and post randomization method are also discussed in detail. The Knowledge Discovery Data Mining Techniques to Preserve Privacy such as k-anonymity, Advanced Traveler Information Systems (ATIS) and Geographical Information System (GIS) are elaborately studied . Partition-And-Group Framework for Clustering Trajectories *TRACLUS* algorithm, secure verification proof gathering protocol (SLVPGP) and a large-scale quantitative analysis of Brightkite, a commercial location-based social network (LSN) are also elaborately studied. Decentralization Methods to Preserve Privacy Dummy Node and Cloaking Region Security Methods and Location Based Services for Securing Moving Data Objects are portrayed.

KEYWORDS: Computer Based Medical Healthcare System, Computerized Medical Diagnosis, Neural Network, Automated Patient Identifier, Cloud Computing.

I. INTRODUCTION

Now-a-days we can note many spreading 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 collects many temporal data to cover sensational massages of an organization and especially he/she can discover many personal information of third party/check points of many premises. Typically personal data (data privacy) are been fetched. Due to user's identity replacement which is actually like terminal i.e. QID is a 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. Even though the location privacy has already been accepted as an important problem and effective privacy-preserving solution is 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. 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)
2. Quick & Efficient discovery of QID of moving data objects

The remainder of the paper is organized as follows. Section 2 deals about Data Disclosure Preventing Techniques. Privacy Homomorphism and Encryption Methods is discussed in Section 3. Section 4 portrays the Knowledge Discovery Data Mining Techniques to Preserve Privacy. Partition-And-Group Framework for Clustering Trajectories is dealt in Section 5. Section 6 briefs about Decentralization Methods To Preserve Privacy Dummy Node and Cloaking Region Security Methods are discussed in detail in Section 7. Section 8 details about Location Based Services for Securing Moving Data Objects. Section 9 concludes the paper and outlines the direction for Future Work

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

II. DATA DISCLOSURE PREVENTING TECHNIQUES

In 1986 [3], the author says that the demographical bureau utilize different disclosure preventing techniques with ad-hoc approval publishing data. Based on the predictive distributions and the uncertainty functions the issues in the general disclosure limiting (DL) approach is been illustrated. In the paper (1987) [4], the author exposed that the information or details about a particular person is been collected for one purpose and it is been used for some other purpose. For example, an Intruder is collecting the information about the person for storing his details in a bank. In turn the intruder will also attain the further information about a person while claiming the money from him. By this the intruder can able to know the actual expenditure of the users.
In 1988 [5], the author's had a debate about whether the researchers are required to give others the data and also the standard procedure on sharing the data. In 1989 [6], the author said that the purpose of this article is that to recognize two specific things to protect the personal information is confidence and privacy. The author says in 1990, that the need of protection towards the privacy of data is not been known till we experience it. The author also compares the privacy with freedom. In 1991 [7], the author said that contributing extended care is the fundamental goal for nursing and searching path to assure to go on at critical focus. Different techniques and methods are developed continuously for evaluating the efforts. As the security of the data is been increased, the patient data will be kept in a very confidential manner which requires larger computerized system for storing and retrieval of data.
In 1992 [8], the author mentioned that the privacy breach all over the world have been progressively developed familiar factor that are global in nature and the privacy establishment has generally been persist at a national level. The first successful attempt to create a universal method towards privacy protection was done by the formation of Privacy International (PI) in Washington DC in March 1992. There was a steady increase in the surveying of privacy and data protection measure in least 1970's.

III. PRIVACY HOMOMORPHISM AND ENCRYPTION METHODS

In 1993 [9] the author mentioned that Council of Europe is presently seeing for a mandate that would adjust data protection laws all over the European community. If this thing is argued then this mandate would alter exchanges of personal data among European countries and the United States. This article says that the scheduled Data Protection Directive will inturn enhance the American Privacy laws. In 1994 [10], the author proposed a Commercial Masking facility algorithm (CDMF). This algorithm describes a specific method for the confidentiality of the data which uses the Data Encryption Algorithm (DEA) as the fundamental cryptography algorithm. In 1995[11], the author mentioned that several countries have proposed various principles to protect individual from the intrusion. In 1996[12], the author introduced a privacy homomorphism (PH) which has different method of illusive privacy across a known clear text attack. The additive and multiplication privacy homomorphism which is an encryption function performs addition and multiplication of plaintext data into two operations on encrypted data. The privacy homomorphism is a tool for converting plain text to encrypted text.
In 1997 [13], the author mentioned that there is a great constraint for providing the personal information. The basic method is to give disclosure-limited data which increase its statistical usage to confidential constraints. The author examined the essential uncertainty in real data with the help of disclosure limitation based on Markov Chain method. An extension of PRAM (post randomization method) called Markov Perturbation is proposed in order to use with categorical data table. It permits cross-classified marginal totals to be preserved and guarantee to give extra information than the usually utilized cell suppression technique. The firm which contains the information has to intent the problem between the requirement by data subject and also the providers for providing the privacy and confidentiality. These firms have two essential tools as follows

1) Restricting access which limits or have a constraint over the data for accessing it.
2) Restricting data which provides access to data which is been converted to minimize the risk of disclosure of individual attributes of data subjects.

IV. KNOWLEDGE DISCOVERY DATA MINING TECHNIQUE TO PRESERVE PRIVACY

In 1998 [14], the author said that nowadays the publishing and sharing of personal data on social places are great demand and the historical data is been available electronically. The statistical information is also available which encounter the information microscopically detailed transaction. While these datum are joined then they give an

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

electronic shadow of a particular person or an firm which are used for identifying the information even it does not contain the explicit identifiers like name, mobile number and address inorder to protect the anonymity of individual data. The data other than these are said to be as Quasi-identifier (QI) usually integrate uniquely identifies and it can linked to the information available publically inorder to re-identify the individuals. In this paper, the author addressed the problem of disclosing person's particular data also protecting the anonymity of a particular person to whom the information is used to refer. This proposal is based on the definition of k-anonymity, where QI group should contain atleast k-1 rows which are identical to each other. The author also introduced a concept of minimal generalization. In this method, it identifies the features of the disclosed process which is not to show the data more than required inorder to achieve k-anonymity.

In 1999 [15], the author introduced a technology called Knowledge Discovery and Data Mining (KDDM) for some of common issues like secondary use of the personal information, handling misinformation and granulated access to personal information. This also has discussed about the new security threats awkward KDDM which contains large collection of data, data warehouses, statistical analysis and consequent learning technique.

In 2000 [17], the author explains about the concept of Advanced Traveler Information Systems (ATIS) which requires easy information retrieval and updating in a dynamic environment at different geographical scales. This ATIS application is helpful in obtaining the improved usage of the limited costly transportation arteries and giving the information about the value-added traveler. This ATIS does not need any additional requirements like real-time response because it is been built on the features given by the Geographical Information System (GIS).

V. PARTITION-AND-GROUP FRAMEWORK FOR CLUSTERING TRAJECTORIES

In 2001 [18], the author presented a new query processing technique for trajectory data stemming from a constrained movement scenario. The extended the well-known two-step technique from spatial query processing to include an additional pre-processing step prior to the filter step. Given an arbitrary spatiotemporal range query, QW, the aim of this step is to segment QW into a set of smaller query windows. Authors exploit infrastructure information, i.e., spatial objects that constrain movement, to segment QW. The rationale is that we "chop" away those parts of QW that range over infrastructure, i.e., those parts of the data space that do not contain trajectory data. In 2002 [19] the author addresses the problem of querying moving objects databases which capture the inherent uncertainty associated with the location of moving point objects and also address the issue of modelling, constructing, and querying a trajectories database. The author proposed to model a trajectory as a 3D cylindrical body. The model incorporates uncertainty in a manner that enables efficient querying. Thus this model strikes a balance between modelling power, and computational efficiency.

In 2003 [20] the author has demonstrated how locations of significance can be automatically learned from GPS data at multiple scales and have also shown a system that can incorporate these locations into a predictive model of the user's movements. In 2004, the author analyses algorithms that suppress location updates and thus hide visits to sensitive areas and introduce the location inference problem—an adversary can infer supposedly hidden locations from prior or future location updates—and present algorithms to address this problem. A synthetic urban mobility model helps us analyse their effectiveness. This paper presents (2005) [21] a preliminary investigation on the privacy issues involved in the use of location-based services. It is argued that even if the user identity is not explicitly released to the service provider, the geo-localized history of user-requests can act as a quasi-identifier and may be used to access sensitive information about specific individuals.

In 2006 [22], the author describes about the privacy preservation. In recent years, the privacy preservation algorithm was developed in order to preserve or safeguard out sensitive information. The disclosure of the context of confidential data is through the exchange of information between each other's and with the help of the information gathered will be useful to obtain the unreleased data. In 2007 [23], the author has proposed a novel framework, the *partition-and-group* framework, for clustering trajectories. Based on this framework, the author have developed the trajectory clustering algorithm *TRACLUS*. As the algorithm progresses, a trajectory is partitioned into a set of line segments at characteristic points, and then, similar line segments in a dense region are grouped into a cluster. The main advantage of TRACLUS is the discovery of common sub-trajectories from a trajectory database.

In 2008 [24], author introduced the novel concept of (k, ±)- anonymity for privacy preserving data publication from moving objects databases, that exploits the inherent uncertainty of location in order to reduce the amount of distortion needed to anonymize data. The rigid pre-processing described could be avoided by adopting a time-tolerant distance function, such as EDR, for the clustering step. Also more sophisticated techniques to handle the trade-off

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

between cluster radius and trash rate are under investigations. In this paper the author assumed a uniform uncertainty level ± for all the moving points. In some applications this could not be the case, and different moving objects could have different uncertainty level ±.

In 2009 [25], the author said that increasing availability of space-time trajectories left by location-aware devices is expected to enable novel classes of applications where the discovery of consumable, concise, and actionable knowledge is the key step. However, the analysis of mobility data is a critic task by the privacy point of view: in fact, the peculiar nature of location data might enable intrusive inferences in the life of the individuals whose data is analysed. It is thus important to develop privacy-preserving techniques for the publication and the analysis of mobility data. In the same year 2009b, the author proposed a system for verifying the location claims by comparing the proofs collected from the neighbouring devices and also introduced a protocol in order to safeguard this proof collecting process, preserving the privacy of all belonging users and protecting it from the malicious users or hackers or intruders and also malicious devices. Even though the application can be extended up to any device with wireless and cryptographic features, a protocol has been developed to functions within the area of vehicular networks called secure verification proof gathering protocol (SLVPGP). In the same year 2009c, 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. On the other hand, women users are younger than their male peers. Based on the patterns of users' location clusters, we can classify users' mobility patterns into four mobility groups. The social graph for Brightkite is fairly sparse since it is an early stage service, though the degree distribution still follows the power law.

In 2010a [26], the author proposed a framework for location privacy that unifies its relevant components, considering users' actual location-privacy requirements. The author identifies various categories of threats, and establishes a methodology for measuring location privacy in different scenarios in order to identify appropriate location-privacy metrics. In the same year 2010b [27], the author said that the contribution of anonymity in relational databases has fascinated a great deal of concentration in the database community during the last decade. Among the various solution methods that have been proposed to tackle this problem, *K*–anonymity has received additional attention and has been extensively studied in different forms. New forms of data that come into existence, like location data capturing user movement, pave the way for the offering of cutting edge services such as the prevailing Location Based Services (LBSs). In the same year 2010 c [28], the author stated that he studied the problem of publishing movement data while preserving the privacy and proposed a method that combines a well-known notion of k-anonymity and a technique for the spatial generalization of trajectories. In particularly he introduced two k-anonymization strategies. The novelty of these approaches lies in finding a suitable tessellation of a geographical area into sub-areas depending directly of the input trajectory dataset.

VI. DECENTRALIZATION METHODS TO PRESERVE PRIVACY

The extension of mobile devices in 2011 a [29], 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). Although LBS provide valuable services for mobile users, exposing their private locations to potentially untrusted LBS service providers pose privacy concerns. In general, there are two types of LBS, namely, snapshot and continuous LBS. In the same year 2011 b [30], 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. In the same year 2011 c [31], 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). Although LBS provide valuable services for mobile users, exposing their private locations to potentially untrusted LBS service providers pose privacy concerns. In general, there are two types of LBS, namely, snapshot and continuous LBS. For snapshot LBS, a mobile user only needs to report its current location to a service provider once to get its desired information.

In 2012 a [32], the author said that the Privacy protection has recently received considerable attention in location-based services (LBS). A large number of location cloaking algorithms have been proposed for protecting the location privacy of mobile users. In this paper, the author considered the scenario where different location-based query requests are continuously issued by mobile users while they are moving. They mentioned that most of the existing k-anonymity location cloaking algorithms are concerned with *snapshot* user locations only and cannot. In the same year

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

2012 b [33], the author stated that with the increasing importance of user location privacy issues, many techniques have been proposed to guard mobile users' location information. However, it is observed that these existing approaches usually assign that users' privacy requirements are *constant*, which may not always be true in real-life scenarios. In this paper, observing that a mobile user's privacy requirements can be dynamic and diverse, which is been said as the L2P2 problem. In the same year 2012 c [34], 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). In this paper, the author stated that they have proposed a game-theoretic framework that enables a designer to find the optimal LPPM for a given location-based service, ensuring a satisfactory service quality for the user. 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.

VII. DUMMY NODE AND CLOAKING REGION SECURITY METHODS

In 2013 a [35], the author said that nowadays the highly accurate positioning devices furnish the user to give different types of LBS which contains keen information of a person and the disclosure of this information will cause a problem. Though several techniques like dummy node concept and cloaking-region (CR) concept had decreases the quality of service (Qos) while the anonymity is increased and vice versa. In the same year 2013 b [39], authors shows the present utilization of uncertainty information in a selection of applications in a mobile and also shows the possibility of introducing artificial uncertainty into location information while using LBS without illustrating it. In the same year 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 proposal principle will inturn increases the lifetime of wireless sensor network (WSN) which relay on the nodes with high energy consumption or hotspot.

VIII. LOCATION BASED SERVICES FOR SECURING MOVING DATA OBJECTS

In 2014 a[41], the author mentioned that the recent mobile devices has an integrated position sensors which may have serious problem if these positions are not protected frequently and is compulsory to ensure the user's acceptance of LBS. Inorder to safeguard user position, an approach called location obfuscation is used which slowly decreases the precision of a positions and so the intruder can get only the information about the coarse grained position. In the same year 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. Due to the LBS provider discloses it data to a 3rd party who process users LBS query, the FINE approach adopts the Data-as-a service (Daas) mode. In order to achieve fine-grained access control, privacy of location, confidentiality of the LBS data and exact LBS query output without allowing my Trusted Third Party (TTD), the FINE framework employs a cipher-text-policy anonymist attribute based encryption (CP-AABE) technique. In the same year 2014 c[43], the author stated that the LBS have become a important part of our regular life. Because of the untrusted LBS server user's may lose the privacy even though it is been utilized the features of LBS by the users regularly. 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.

IX. CONCLUSION AND FUTURE WORK

Various methods to protect moving data objects for the past 30 years is discussed. The paper dealt about the development of Early data object protection methods which are rooted since 1984. Data Disclosure Preventing Techniques such as disclosure limiting and ad-hoc approval publishing data are depicted. Privacy Homomorphism and Encryption Methods such as Data Protection Directive, Commercial Masking facility algorithm, Data Encryption Algorithm and post randomization method are also discussed in detail. The Knowledge Discovery Data Mining Techniques to Preserve Privacy such as k-anonymity, Advanced Traveler Information Systems (ATIS) and Geographical Information System (GIS) are elaborately studied. Partition-And-Group Framework for Clustering Trajectories *TRACLUS* algorithm, secure verification proof gathering protocol (SLVPGP) and a large-scale

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

quantitative analysis of Brightkite, a commercial location-based social network (LSN) are also elaborately studied. Decentralization Methods To Preserve Privacy Dummy Node and Cloaking Region Security Methods and Location Based Services for Securing Moving Data Objects are portrayed. This survey would promote a lot of research directions in the field of 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, PrisclaM. "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 : 3-10, 2010.
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 : 91-121, 2010.
32. Chow, Chi-Yin, and Mohamed F. Mokbel. "Trajectory privacy in location-based services and data publication." *ACM SIGKDD Explorations Newsletter* 13, no. 1: 19-29, 2011.

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

33. Hashem, Tanzima, and Lars Kulik. ""Don't trust anyone": Privacy protection for location-based services." *Pervasive and Mobile Computing* 7, no. 1: 44-59, 2011.
34. Bonchi, Francesco, Laks VS Lakshmanan, and Hui Wendy Wang. "Trajectory anonymity in publishing personal mobility data." *ACM Sigkdd Explorations Newsletter* 13, no. 1: 30-42, 2011.
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 : 1506-1519, 2012.
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: 633-651, 2014.
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: 163-175, 2014.
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.

BIOGRAPHY

P.Andrew J.Anish kumar 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, Amsterdam 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.**