ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

Survey on Approaches Developed for Preserving Privacy of Data Objects

P.Andrew[1], J.Aneesh[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, L&T Infotech, Chennai, TamilNadu, India[5]

Abstract: This paper reviews methods to secure objects for the past 30 years. Data Disclosure Preventing Techniques such as uncertainty function and two data transformation technique are depicted. Privacy Homomorphism And Encryption Methods such as Commercial Masking facility algorithm (CDMF), markov-like perturbation and decryption of perturbation are also discussed in detail. The Knowledge Discovery Data Mining Techniques to Preserve Privacy such as generalization, suppression are elaborately studied. Partition-And-Group Framework for Clustering Trajectories TRACLUS algorithm, natural spatio-temporal operators are also elaborately studied. Decentralization Methods to Preserve Privacy location including k-anonymity and cloaking granularity as privacy metrics, a new incremental clique-based cloaking algorithm, called ICliqueCloak, to defend against location dependent attacks was discussed. Dummy Node and Cloaking Region Security Methods and Location Based Services for Securing Moving Data Objects are described

Keywords: Data Disclosure, Encryption, Knowledge Discovery Data Mining, spatio-temporal databases, database privacy

I. INTRODUCTION

Recent days have seen 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. Many author's had undergone many survey's and created their algorithms. 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. [2009] [44] 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 increase the request are deferred/postdated. As the velocity increases the request for temporal data should be processed while moving.

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.

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 outline the direction for Future Work.

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

II. DATA DISCLOSURE PREVENTING TECHNIQUES

In 1986 [3] paper, the author says that the demographical bureau utilize different disclosure preventing techniques with ad-hoc approval publishing data. The situation on a target with the user's data is been shown by one predictive distribution before and after the data release. The lagging of user's knowledge about the target is been calculated using uncertainty function. The disclosure of data is been minimized with a two data transformation technique like aggregation and suppression[1] [2].

In 1987 [4] this paper, 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. The sole aim of collecting information about the user is for the sake of bank and it is been utilized in an unauthorized way. As like this the hospital information, social security databases, police files, subscriber profile etc..is been misused. In order to provide the security to the unauthorized access of public data, a social security number (SSN) is provided which is used to identify the illegal and ineligible persons.

In 1988 [5], the author had a debate about whether the researchers are required to give others the data and also the standard procedure on sharing the data which is been developed by American Psychological Association and other organizations are inspected. The constitutional indication of ethical principles of authorizing data sharing is also recorded.

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.

In 1990 [7], the author says 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 [8], the author said that contributing extended care is the fundamental goal for nursing and searching path to assure to go on at critical focus. 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. Though the privacy mechanisms are increasing, the author also takes two applicable approaches are taken into consideration. They are "the right of the individual to control the amount of information he/she divulges about him" and "the capacity of the individual to determine which information has to be controlled".

In 1992 [9], 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 groundwork for this privacy principle is developed by OECD and the Council of Europe. The European commission has freshly formed a draft directive for application in the public and private sectors through the United Nations have still to formulate particular delegates. The Non-Government Organizations (NGOs) have played a least role in the evaluation of international protection of privacy and it is also involved in privacy protection has presently be confined to national feedbacks.

III. PRIVACY HOMOMORPHISM AND ENCRYPTION METHODS

In 1993 [10], the author mentioned that Council of Europe is presently seeing for a mandate that would adjust data protection laws all over the European community. This will not arise as an easy reaction to an anticipated economic threat but due to several numbers of social economic and potential changes in the privacy conditions in the United States concur at present. The European Directive provide a hope for agreement change to happen but will not be the cause of the change.

In 1994 [11], the author proposed a Commercial Masking facility algorithm (CDMF). This algorithm abates the entire cryptographic operation by providing a key-generation technique that in-turn produces and valuate 40-bit DEA key in spite of 56-bits which is been required by full-strength DEA. Normally, this algorithm is said to be a drop-in replacement for the DEA in cryptographic produces.

In 1995 [12], the author mentioned that several countries have proposed various principles to protect individual from the intrusion. The Organization for the Economic Corporation and Development (OECD) has a particular guidelines related to data privacy that formally affect those underlying knowledge discovery and also to those which use personal data.

In 1996 [13], the author introduced a privacy homomorphism (PH) which has different method of illusive privacy across a known clear text attack. Initially, it is an encrypted function Ek *: T + T'* that permits to develop a set *F'* of actions on encrypted data without the ability of the decryption function Dk and the scope of Dk grant to recollect the output of the belonging set F' of operation of operations on plain text. This PH involves two important developments which are as follows

-- Small values are nontrivially encrypted
-- The new PH is able to combat a known clear text attack.

The author concluded by producing an application of the proposed PH to multilevel estimating on sensitive data. With PH a classified level can disclose privacy protected data. When the classified level retrieves the result of a computation from the unclassical level to obtain the exact result, the decryption of perturbation takes place and it adds the clear perturbation to the perturbed result.

In 1997 [14], the author focused mainly for protecting the "unbiasedness" of the post randomization perturbations particularly with regard to zero cell entries. Protecting the zero entries in this situation will result to non-existence of a markov-like perturbation. In order to view these tables

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

is to inspect "interchanging" the zeros and ones with same Markov like procedures with respect to marginal constraints, this will then in turn change unbiasedness to the lower order margins. The Markov perturbation method will prevent the disclosure of categorical data. It gives additional information to valid or authentic data user than cell suppression. AS like every disclosure limitations method it requires the following,

(1) Time and keen attention to implement and work with the technique.
(2) It arises queries on consistency while the similar tables are released.

The noise is to be voluntarily introduced through the Markov perturbation method which is said to be misclassification error and it is been handled only by the experienced data analyst.

IV. KNOWLEDGE DISCOVERY DATA MINING TECHNIQUE TO PRESERVE PRIVACY

In 1998 [15], the author showed how k-anonymity can be ensured in data disclosure by generalization or suppression and part of the data to be leaked. Generalization has the advantage of allowing disclosure of all the single tuples in the table in a general form. Suppression is to remove data from the table so that they are not released. It is used to moderate the generalization process in order to limit the tuples with less than K-occurrences. The possible preference polices are used to choose among various minimal generalization and an algorithm to calculate a suitable minimal policies. The author put forth his work to be considered is about to determine the quality and usefulness in other settings. He also suggested some future work of multiple releases overtime, data updating etc which may allow inference attacks. In 1999 [16] paper, 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. It also uses a large amount of data to produce hypothesis and introduce general patterns. This KDDM incorporates some new challenges to security like stertotypes, safeguarding personal or confidential data from KDDM researchers, individuals from training sets and combination of patterns. KDDM describes various activities and methods for extracting information from data and suggesting patterns in huge databases.

In 2000 [17], the author investigates the utilization of a network of computers for resolving complicated problems and privacy preservation for sensitive data. The system architecture composing of a central site, a set of base stations, non-mobile computers hanged up to the system through some medium. In order to represent the ATIS information, new data models like relational object oriented model and temporal relational object oriented models are introduced which permit us to represent static and dynamic information. The information is held up in spatial and temporal domains. The author informed that these model has some limitations like lack of standard and efficient query language for OODB, network bandwidth, failure in the central site etc.. he also suggested some solutions and reasons for the failure of this model is like that a keen research is been carryout for better understanding, the limited storage with the network bandwidth will be resolved by the next generation gigabit networks.

V. PARTITION-AND-GROUP FRAMEWORK FOR CLUSTERING TRAJECTORIES

In 2001 [18], the author devised an algorithm for segmenting the QW based on infrastructure. This segmentation can have three outcomes. Query processing can be (i) stopped after the pre-processing step, i.e., QW is totally covered by infrastructure, (ii) QW is segmented into a set of smaller query windows which is used for querying the trajectory data, or (iii) the original range query is used. Case (i) is easy to decide. For cases (ii) and (iii), it depends on heuristics that are based on the outcome of the segmentation process. The results of the performance studies reported give a first indication for such heuristics. Although recent literature includes work on indexing trajectories of moving objects by maintaining the complete history of object movement the work presented in this paper is the first (i) to propose a query processing technique tailored towards trajectory data stemming from objects moving in scenarios constrained by infrastructure, and (ii) to use a pre-processing step that is based on data other than approximations of the trajectory data This works points to several directions for future research. Using the outcome of the segmentation process directly might not be the most favourable choice.

In 2002 [19], the authors demonstrated efficiency, relate the length of a trajectory to its size in bytes. The experiments were conducted using a real map of the Chicago Metropolitan area. The author in turn introduce a set of novel but natural spatio-temporal operators which capture uncertainty, and are used to express spatio-temporal range queries also devise and analyse algorithms to process the operators. The operators have been implemented as a part of our DOMINO project. 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 addition, they have described several potential applications of such models, including both single and multi user scenarios. Potentially such methodologies might be extended to other sources of context as well.

In 2004 [21] this article, 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.
In 2005 [22] paper presented a preliminary investigation on the privacy issues involved in the use of location-based

ISSN 2393-8021

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 2, October 2014

services. The paper formally defines a framework to evaluate the risk in revealing a user identity via location information and presents preliminary ideas about algorithms to prevent this to happen. In 2006 [23], the author describes about the privacy preservation. 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. For these problem, a Bayesian network based mechanism is been developed. This algorithm has some disadvantage namely the data may be a historic data which may differ from day-to-day life and thus the data stored in this problem was static. So to overcome this problem, the author proposed new mechanism called dynamic Bayesian network which assures safe data release.

In 2007 [24], 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*. The main advantage of TRACLUS is the discovery of common sub-trajectories from a trajectory database. To show the effectiveness of TRACLUS, the author has performed extensive experiments using two real data sets: hurricane track data and animal movement data. The heuristic for parameter value selection has been shown to estimate the optimal parameter values quite accurately. They also have implemented a visual inspection tool for cluster validation. The visual inspection results have demonstrated that TRACLUS effectively identifies common sub-trajectories as clusters.

In 2008 [25] author introduced the novel concept of (k, ±)-anonymity for privacy preserving data publication from moving objects databases. Their method can be straightforwardly extended to deal with this situation by taking, for each cluster, the minimum ± appearing in the cluster (but more sophisticated techniques could be devised). It has been recently recognized and in many other works, that k-anonymity alone does not put us on the safe side, because although one individual is hidden in a group, if the group has not enough diversity of the *sensitive attributes* then an attacker can still associate one individual to sensitive information. However, in the context of moving object data the problem is very challenging, because position is a different kind of information that could be considered to be sensitive and quasi-identifier at the same time. Therefore, since anonymity requires similarity on the quasi identifiers, and diversity requires dissimilarity on the sensitive information, it seems that in the case of moving object data they are two conflicting goals. Finally, In this paper the author informed that they did not consider any concept of quasi-identifier for trajectories, and thus they did not tackle the diversity problem: these are interesting and open research problems that deserve deep investigation.

In 2009a [26] the author provided a brief survey of the research on *anonymity preserving data publishing of moving objects databases*. While only few papers so far have tackled the problem of anonymity in the off-line case of publication of a moving objects database, rather large body of work has been developed for anonymity on relational data on one side, and for location privacy in the on-line, dynamic context of *location based services* (LBS), on the other side. In 2010a [29], the author proposed framework laid a future work for us to design and build appropriate location-privacy protection mechanisms, identify the drawbacks of existing works, express different works with the same terminology, and discover new directions for research in location privacy.

VI. DECENTRALIZATION METHODS TO PRESERVE PRIVACY

In 2011a [32] authors spoke that, 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. The author also informed as that, it is expected to have more effective and efficient privacy preserving technologies will be developed in the near future. The author also provided some future directions in these two problems as the conclusion of this survey. For continuous LBS, new privacy-preserving techniques are needed to protect personalized LBS. This is because personalized LBS require more user semantics rather than just some simple query parameters, such as a distance range and an object type of interest. An adversary could use such user semantics to infer the user location with higher certainty. Existing privacy-preserving techniques for location trajectory publication only support simple aggregate analysis, such as range queries and clustering. Researchers should develop new trajectory anonymization techniques that support more useful and complex spatiotemporal queries and data analysis.

In 2012a [34] the author said that the Privacy protection has recently received considerable attention in location-based services (LBS). They mentioned that most of the existing k-anonymity location cloaking algorithms are concerned with *snapshot* user locations only and cannot effectively prevent location-dependent attacks when users' locations are continuously updated. Therefore, adopting both the location k-anonymity and cloaking granularity as privacy metrics, the author proposed a new incremental clique-based cloaking algorithm, called ICliqueCloak, to defend against location dependent attacks. The main idea is to incrementally maintain maximal cliques needed for location cloaking in an undirected graph that takes into consideration the effect of continuous location updates. Thus, a qualified clique can be quickly identified and used

to generate the cloaked region when a new request arrives. The efficiency and effectiveness of the proposed ICliqueCloak algorithm are validated by a series of carefully designed experiments. The experimental results also show that the price paid for defending against location-dependent attacks is small. The average processing time is only 5.7*ms* and the cloaking success rate is about 97% for most cases, which checks the efficiency and effectiveness of the proposed IClique-Cloak algorithm.

VII. DUMMY NODE AND CLOAKING REGION SECURITY METHODS

In 2013 a [38], the author said that 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 this paper, the author presented a node density-based location privacy method which will give the location security by using the hybrid concept of dummy node and cloaking-region and this result shows that the probability of tracing the targeted node by an intruder is been reduced and also the QoS of LBS will inturn increased.

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. The model reduces the attacker's action still the attacker hack the information with the help of the map matching to increase the precision of the already known position. To protect the user identity k-anonymity algorithm is used and also it is based on a Trusted Third Party (TTD) for anonymization. The main aim of this paper is to classify the existing location privacy methods which takes the hackers knowledge and the attacked methods into account and also lists the various protection goals.

IX. CONCLUSION

Various methods to secure data objects for the past 30 years is discussed. The paper dealt about the development of Early data protection methods which are rooted since 1984. Data Disclosure Preventing Techniques such as uncertainty function and two data transformation technique are depicted. Privacy Homomorphism And Encryption Methods such as Commercial Masking facility algorithm (CDMF), markov-like perturbation and decryption of perturbation are also discussed in detail. The Knowledge Discovery Data Mining Techniques to Preserve Privacy such as generalization, suppression are elaborately studied. Partition-And-Group Framework for Clustering Trajectories TRACLUS algorithm, natural spatio-temporal operators are also elaborately studied. Decentralization Methods to Preserve Privacy location including k-anonymity and cloaking granularity as privacy metrics, a new incremental clique-based cloaking algorithm, called ICliqueCloak, to defend against location dependent attacks was discussed. Dummy Node and Cloaking Region Security Methods and Location Based Services for Securing Moving Data Objects are described.

REFERENCES

[1] Solomon, Toby. "Personal Privacy and the 1984 Syndrome." W. New Eng. L. Rev. 7 (1984): 753.
[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 (1986): 10-18.
[4] Simitis, Spiros. "Reviewing privacy in an information society." University of Pennsylvania Law Review (1987): 707-746.
[5] Melton, Gary B. "Must researchers share their data?." Law and Human Behavior 12, no. 2 (1988): 159.
[6] Laster, Daniel. "Breaches of Confidence and of Privacy by Misuse of Personal Information." Otago L. Rev. 7 (1989): 31.
[7] Flaherty, David H. "On the utility of constitutional rights to privacy and data protection." Case W. Res. L. Rev. 41 (1990): 831.
[8] Maciorowski, Linda F. "The enduring concerns of privacy and confidentiality."Holistic nursing practice 5, no. 3 (1991): 51-56.
[9] Davies, Simon G. "Constructing an International Watchdog for Privacy and Data Protection: The Evolution of Privacy International." JL & Inf. Sci. 3 (1992): 241.
[10] Regan, PrisсllaM. "The Globalization of Privacy." American Journal of Economics and Sociology 52, no. 3 (1993): 257-274.
[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 (1994): 217-226.
[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 (1995): 48-59.
[13] Ferrer, Josep Domingo I. "A new privacy homomorphism and applications."Information Processing Letters 60, no. 5 (1996): 277-282.
[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 (2000): 3-15.
[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 (2003): 275-286.
[21] Gruteser, Marco, and Xuan Liu. "Protecting privacy in continuous location-tracking applications." IEEE Security & Privacy 2, no. 2 (2004): 28-34.
[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." InPrivacy 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." InComputational 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 Newsletter12, 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." InINFOCOM, 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.

BIOGRAPHIES

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 10^{th} and 12^{th} 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.