ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

A Survey on Approaches Developed for Data Anonymization

K.Deepika[1], P.Andrew[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 developed for anonymizing data for the past 10 years. Publishing microdata such as census or patient data for extensive research and other purposes is an important problem area being focused by government agencies and other social associations. The traditional approach identified through literature survey reveals that the approach of eliminating uniquely identifying fields such as social security number from microdata, still results in disclosure of sensitive data, k-anonymization optimization algorithm ,seems to be promising and powerful in certain cases ,still carrying the restrictions that optimized k-anonymity are NP-hard, thereby leading to severe computational challenges. k-anonimity faces the problem of homogeneity attack and background knowledge attack . The notion of l-diversity proposed in the literature to address this issue also poses a number of constraints , as it proved to be inefficient to prevent attribute disclosure (skewness attack and similarity attack), l-diversity is difficult to achieve and may not provide sufficient privacy protection against sensitive attribute across equivalence class can substantially improve the privacy as against information disclosure limitation techniques such as sampling cell suppression rounding and data swapping and pertubertation. This paper aims to discuss efficient anonymization approach that requires partitioning of microdata equivalence classes and by minimizing closeness by kernel smoothing and determining ether move distances by controlling the distribution pattern of sensitive attribute in a microdata and also maintaining diversity.

Keywords: Data Anonymization, Microdata, k-anonymity, Identity Disclosure, Attribute Disclosure, Diversity

I. INTRODUCTION

Privacy-An important factor need to be considered while we publishing the microdatas. Usually government agencies and other organization used to publish the microdatas. On releasing the microdatas, the sensitive information of the individuals are being disclosed. This constitutes a major problem in the government and organizational sector for releasing the microdata. In order to sector or to prevent the sensitive information, we are going to implement certain algorithms and methods. Normally there two types of information disclosures they are: Identity disclosure and Attribute disclosure. Identity disclosure occurs when an individual's linked to a particular record in the released Attribute disclosure occurs when new information about some individuals are revealed.(i.e)the released data make it possible to infer the characteristics of an accurately than it would be possible before the data released. The Knowledge of identity disclosure would often allow us to know about attributes disclosure .Once the identity disclosure comes into exists ,the individuals sensitive information is reidentified. Due to the effects of false attributes ,an observer of a release table may incorrectly perceive that an individuals. sensitive attribute takes a particular value. This can harm the individuals even if the perception is incorrect. When the table is released, it present disclosure risk to the individual who are all in table.

The remainder of the paper is organized as follows. Section 2 deals about basic definition and primitives of data anonymization. The principle of k-anonymity is discussed in Section 3. Section 4 portrays the notion of l-diversity. The limitations of l-diversity are dealt in Section 5. Section 6 briefs about the concept of t-closeness. Evolution of Data Anonymization Techniques are discussed in detail in Section 7. Section 8 details about Data Disclosure Prevention Techniques. The application of Data Anonymization Techniques for several spectrum of data such as trajectory data are depicted in Section 9. Section 10 Concludes the paper and outline the direction for Future Work.

II. BASIC PRIMITIVES AND DEFINITIONS

Anonymity is different from what is usual or expected (ie) when we do something , we do not let people know that we are personal who did it and the information. To reduce the disclosure of data, we need to generalize an anonymized table. This anonymized table consist of records that has no. of attributes .

Attributes among itself can be divided into 3 categories

1. Explicit identifiers- Attributes that clearly identifies individuals.
2. Quasi identifiers- Attributes whose values when taken together can potentially identify an individual.
3. Sensitive identifiers- That are attributes needed to be supplied for researchers keeping the identifiers anonymous.

In order to secure data and to limit disclosure it is necessary to measure the risk of a anonymized table. To established this method Samarit[20] and Sweeny[21] introduced k-anonymity, which requires that each equivalence class contains atleast k-records. Though it protects identity disclosure, but it failed to prevent attribute disclosure to overcome this limitation , Machanavajjhala et al[18] introduced "l-diversity". The l-diversity requires that the distribution of a sensitive

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

attribute in each equivalence class has atleast l-well respresented valuesone of the major problem with l-diversity is, it is limited in its assumption of adversarial knowledge.

The assumption about a sensitive attribute generalized the specific background and homogeneity attacks. Also it is necessary to assume all attributes are to be categorical. (ie)(attributes value taken –T/F).In this paper we propose a novel privacy notation called "closeness".

An equivalence class is said to have a t-closeness if the distance between the distribution of a sensitive attribute in this class and the distribution of attribute in the whole table is no more than a threshold t. A table is said to have t-closeness if all equivalence classes have t-closeness. An analysis on data utility shows t-closeness can limit(secure) the amount of useful information that can be extracted from the received data. Hence it is not so efficient. We move to a flexible privacy model called (n-t) closeness. It limits the amount of information on individuals and activeness better privacy than t-closure and l-diversity. (n,t) closure protects the data better while improving the utility of the released data our approach is to limit the identification of micro data by controlling the sensitive attribute distribution of micro data and maintain diversity, using kernel smoothing and either more distance.

III. The Principle Of K-Anonymity

K-anonymity is a simpler form and are easy to understand. K-anonymity is achieved by anonymising the data before release. Here the explicit identifiers are removed. Though it is not enough as the person may know the quasi-identifier values of some individuals already in the table. The knowledge can be either from the personal knowledge or public. In order to secure both explicit and quasi-identifiers, a generalization method is used, in which all the quasi-identifiers are replaced with less specific values but semantically consistent. As a result more records will have the some values for the quasi-identifier(i.e)K-anonymity requires that each equivalence class atleast K-records. In K-anonymity there are two types of attacks they are homogeneity attack and background knowledge attack .we can discuss the homogeneity attack[16].

IV. The Notion of L-Diversity

Since k-anonymity failed to secure the attribute disclosure, machanavajj el al[18] introduced a new privacy notation called"*l-diversity".* An eqivalance class is said to have l-diversity if there are atleast l well represented values for the sensitive attribute .A table is said to have l-diversity if every equivalence class of the table has l-diversity.

Here the technique is the sensitive attribute in each equivalence class is distributed with l-well represented values. Generally there are four types of l-diversity .

1)Distinct l-diversity: To ensure that there are atleast l-distinct values for the sensitive attribute in each equivalence class.

Disadvantages: It does not prevent probabilistic inference attacks.

2)Probabilistic l-diversity: An anonymised table is said to be probabilistic l-diversity if the frequency of the sensitive value in each group is atmost 1/l.

3)Entropy l-diversity:

It is defined by

$$\text{Entropy (E)} = -\sum_{s\in S} P(E,s)\log p(E,s)$$

Where e S is the sensitive attribute.

4)Recursive(c,l) diversity: It makes the technique by, the value appearing most frequently does not appear too frequently and less frequency value do not appear too rarely.

V. Limitations of L-diversity

One problem with l-diversity is that it is limited in it's assumption of adversarial knowledge. l-diversity failed to prevent attribute disclosure in the field of following two attacks.

a. Skewness Attack:

Skew-It is changed or affected to some extent by a new or unusual factor and so is not correct. Here when the overall distribution is skewed, by satisfying l-diversity, it does not prevent attribute disclosure.

Table 1. Original table before attack

	ZIPCODE	AGE	SEX	DISEASE
1	47665	29	M	VIRAL
2	47602	27	M	CANCER
3	47643	26	M	VIRAL
4	47908	52	M	HEART DISEASE
5	47942	47	F	FLU
6	47932	30	M	HEART DISEASE

In this case,2 diversity does not provide sufficient privacy protection on any one in the class would be 50 percent possibly of being male as compared with 1 percent overall population. In this case, this equivalence class has exactly 49 percent of male and 1 percent of female even though the two classes present very different levels of privacy risk. Hence, if the sensitive attribute in the table is very large, if any one use entropy l-diversity, then they can easily gain the details of data using disclosure and large value of l. Hence l value must be small in order to prevent attribute disclosure.

b. Similarity Attack:

It is possible that in table to have two or more sensitive attribute. For example, consider the following table.

Table 2: Original Table Before Attack

	ZIPCODE	AGE	SALARY	DISEASE
1	47665	29	3K	VIRAL
2	47602	27	5K	CANCER
3	47643	26	4K	VIRAL
4	47908	52	6K	HEART DISEASE
5	47942	47	7K	FLU
6	47932	43	8K	HEART DISEASE

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

Table 3: 3-diverse version of table.

	ZIPCODE	AGE	SALARY	DISEASE
1	476**	<30	3K	VIRAL
2	476**	<30	5K	CANCER
3	476**	<30	4K	VIRAL
4	479**	>=40	6K	HEART DISEASE
5	479**	>=40	7K	FLU
6	479**	>=40	8K	HEART DISEASE

Here, suppose one knows bob's salary in the range of 3-5k,then he can conclude his record correspond to one of the first three records. This leads to leakage of related information (ie)his disease may disclosed. This is happened to have because of diversity of sensitive value in each group of the table. Hence it is necessary to distribute data in some level of diversity providing semantic relationship among them.

VI. Concept of T-Closeness

A positive pregnancy, privacy is measured by the information gain of an observer. Before seeing the released table the observer has think that something happened in the sensitive attribute value of a single person. After seeing the released table the observer may have the details about the sensitive attributes. Here we are going to see about before and after seeing the released table. t-closeness should have the distance between the class and the whole table is no more than a threshold t [15].

VII. Evolution of Data Anonymization Techniques

In (2003) [1] Haoween chan, Perrig.A. said that security and privacy is most important in the case of every applications. Hence it is applicable to sensor networks also. Sensor networks offer economically visible solutions for a variety of applications in the day-to-day life. For example, current implementations, pollution levels, structural integrity of buildings. Other applications include climate sensing and control in buildings etc. hence sensor networks are the key to the creation of smart spaces, which embed information technology in everyday home and work environments. David A.Maltz, Jibin Zhen,Geoffrey Xie, Hui Zheng,Gisli Hjalmytsson, Albert Greenberg ,Jennifer Rexford in (2004) [2] discussed about a collection of router configuration files from production networks contains many information such as network topologies, routing designs, security policies. However, these files has extendable information which are merely sensitive and it can be hacked by competitors and attackers. This paper delivers a method for anonymizing and protecting the router configuration files.

RJ Bayardo,R.Agarwal in (2005) [3] said that data is to be anonymized before they are transmitted. Data de-identification requests the demand for release of data for research purposes and that demand for privacy from individuals. In this paper, the authors proposes and evaluates an optimization algorithm. This algorithm is for the powerful de-identification procedure called as k-anonymization. A k-anonymized dataset is unique. It has the property that each record is indistinguishable from atleast k-1 others.

Jian xu, Wei Wang, Jian pei, Xiaoyuan Wang,Baile Chi, Ada Wai-Chee fu in (2006) [4] stated that privacy becomes more and more serious concern in applications involving microdata. Most of the previous methods use global recoding,which maps the domains of the single attribute to generalized values. Hence global recoding is not at all effective. Different attributes in a dataset may have different utility in the analysis. But in the previous method ,utility attributes has not been considered. In this paper ,the authors studied the problem of utility based anonymization.

Gabriel Ghinita, Panagiotis karras, Panos Kalnis, Nikos Mamoulis in (2007) [5], the author says that sensitive information should not be revealed in the case of privacy. The above specified authors studied the problem of publishing the microdata without revealing the sensitive information by using the two important paradigms like k-anonymity and I-diversity. In the case of k-anonymity, it protects against their identification of an individual record. And in the case of I-diversity, it safeguard against the association of an individual with specific sensitive information. Hence the authors found that their existing approaches suffered from at least one of the following drawbacks i)The information loss metrics are seeming to the right and it fails to capture data inaccuracy for the sake of privacy. ii)I-diversity is solved by k-anonymity, but it introduces unnecessary inaccuracies. iii)The anonymization process is not efficient in the sake of computation and input and output cost.

VIII. Data Disclosure Prevention Techniques

Tiancheng Li, NingLui Li in (2008) [6] Agencies and other organizations often need to publish micro data. Those microdata should be guard as a sensitive information. Existing work on privacy preserving data publishing cannot satisfactorily prevent an conflicts with background knowledge. But the background knowledge will be useful in learning important sensitive information. Background knowledge attack is due to additional knowledge. The authors found that recent work has shown that background knowledge attack on present disclosure risks to the secured data. No work has used background knowledge in data anonymization. TianCheng Li, NingLui Li, Jian Zheng in (2009) [7] portrayed that there are a number of privacy models have been proposed for data anonymization. The authors say that the recent work has shown the importance of consisting the opponent's (adversary) background knowledge when reasoning about privacy is data publishing. Hence, it seems to be very difficult for the data publisher to know exactly the adversary's background knowledge. The injector approach considers only the background knowledge and does not provide an approach to analyze how an adversary can gain sensitive information from the published data.

Das.S, Egecioglu.O, EL Abbadi.A in (2010) [8] depicts that social networks plays a major role in today's world. The social networks popularity initiated a fertile

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 1, Issue 3, November 2014

research area in Information extraction and data mining. Hence such analysis can facilitate better understanding of sociological,behavioral and other interesting phenomena. Hence these analysis require effective anonymization techniques. In this paper ,the authors considered edge weight anonymization in social graphs. Their approach builds a linear programming(LP) model.

Noman Mohammed, Ruichen, Benjamin C.M.Fung, Philip S.Yu. in (2011 a) [9] Privacy preserving data has many disclosure drawbacks. It addresses the problem of disclosing sensitive data. There are many existing privacy models. In that €-differential privacy provides one of the strongest privacy. but it has no assumptions about an opponent's background knowledge. Mostly ,the existing solutions that ensure €-differential privacy are based on an interactive model.

Jianneng cao, Carminati.B, Ferrari.E, Tan KL in (2011 b) [10] say that there are many privacy preserving methods are in existence methods such as k-anomity are designed only for static datasets. But,they cannot be applied to streaming data. Streaming data refers to the continuous,transient andusually unbounded datasets. In streaming applications,it is a mandatory to offer strong guarantees on the maximum allowed delay between incoming data and the corresponding anonymized output.

Aris Gkoulalas-Divanis, Grigorios Loukides in (2011 c) [11] the case of biomedical studies,the transaction data about individuals are collected. Publishing these datas are required by many organizations. But it may result in privacy problems. Algorithms that prevent this threat by transforming transaction data have been proposed recently. But that method doesn't meet each and every requirements,owners need. To address this problem,the authors proposed a clustering based framework to anonymizing data while transaction.

IX. DATA ANONYMIZATION FOR TRAJECTORY DATA

Tamersoy.A, Loukides.G, Nergiz.M.E, Saygin.Y,Malin.B in (2012) [12] tells that data is anonymized not only for the transactions but also used in medical issues. Electronic Medical Record[EMR] systems have enabled healthcare providers to collect the detailed information of the patients. In the case of clinical decision in hospitals, longitudinal data from EMRs are increasingly combined with bio-repositories. Emerging policies encourage investigators to prepare such data in a de-identified form to reuse and collaborate,but organizations are hesitant to do so. As because they fear such actions will confuse patient privacy.

Poulis.G,Skiadopoulos.S,Loukides.G,Gkoulalas-divanis.A. in (2013) [13] discusses the publication of moving data(trajectory data) opens up new directions in studying human behavior. But it is challenging to perform in a privacy preserving way. This is mainly because, the identities of individuals, whose movement is recorded in the data, can be disclosed even after removing identifying information. There are some existing works which preserve privacy, but at a high data utility cost.

Burke.M.J, Kayem.A.V.D.M in (2014) [14], depicts the case of crime branches, mobile crime report services have become a vast approach to enable community based crime reporting(CBCR) in developing nations. These services hold the advantages of facilitating law enforcement when resource constraints make using standard crime investigation approach. But CBCRs failed to achieve widespread popularity because of privacy. users become hesitant to make crime reports without privacy preservation.

X. CONCLUSION

Various methods developed for anonymizing data for the past 10 years are discussed. Publishing microdata such as census or patient data for extensive research and other purposes is an important problem area being focused by government agencies and other social associations. The traditional approach identified through literature survey reveals that the approach of eliminating uniquely identifying fields such as social security number from microdata, still results in disclosure of sensitive data, k-anonymization optimization algorithm ,seems to be promising and powerful in certain cases ,still carrying the restrictions that optimized k-anonymity are NP-hard, thereby leading to severe computational challenges. k-anonimity faces the problem of homogeneity attack and background knowledge attack . The notion of l-diversity proposed in the literature to address this issue also poses a number of constraints , as it proved to be inefficient to prevent attribute disclosure (skewness attack and similarity attack), l-diversity is difficult to achieve and may not provide sufficient privacy protection against sensitive attribute across equivalence class can substantially improve the privacy as against information disclosure limitation techniques such as sampling cell suppression rounding and data swapping and pertubertation. Evolution of Data Anonymization Techniques and Data Disclosure Prevention Techniques are discussed in detail. The application of Data Anonymization Techniques for several spectrum of data such as trajectory data are depicted. This survey would promote a lot of research directions in the area of database anonymization.

REFERENCES

[1] Haoween chan, Perrig.A," Security and privacy in sensor networks", published in computer Volume 36, Issue:10, 2003.
[2] David A.Maltz, Jibin Zhen,Geoffrey Xie, Hui Zheng,Gisli Hjalmytsson, Albert Greenberg ,Jennifer Rexford "Structure preserving anonymization of router configuration data", published in 4th ACM SIGCOMM conference on internet measurement, 2004.
[3] RJ Bayardo,R.Agarwal ," Data privacy through optimal k-anonymization" published in 21st International conference,2005.
[4] Jian xu, Wei Wang, Jian pei, Xiaoyuan Wang,Baile Chi, Ada Wai-Chee fu," Utility based anonymization using local recording",published in 12th ACM SIGKDD International conferences on knowledge discovery and data mining, 2006.
[5] Gabriel Ghinita, Panagiotis karras, Panos Kalnis, Nikos Mamoulis," Fast data anonymization with low information loss", published in 33rd International conference on very large databases,2007
[6] Tiancheng Li, NingLui Li," Injector: Mining Background Knowledge for data anonymization",published in 24th International conference on Data Engineering,2008.
[7] TianCheng Li, NingLui Li, Jian Zheng,"Modeling and integrating background knowledge in data anonymization" published in 25th International conference on Data Engineering, 2009.

[8] Das.S, Egecioglu.O, EL Abbadi.A," Anonymizing weighted social network graphs", published in 26th International conference on Data Engineering,2010.
[9] Noman Mohammed, Ruichen, Benjamin C.M.Fung, Philip S.Yu," Differentially private data release for data mining, ACM SIGKDD International conferences on knowledge discovery and data mining,2011 (a).
[10] Jianneng cao, Carminati.B, Ferrari.E, Tan KL," CASTLE: continuously anonymizing data streams", published in dependable and secure computing,(volume:8,issue:3),2011 (b)
[11] Aris Gkoulalas-Divanis, Grigorios Loukides," Privacy –constrained clustering-based transaction data anonymization",published in 4th International workshop on privacy and anonymity in the Information society,2011 (c)
[12] Tamersoy.A, Loukides.G, Nergiz.M.E, Saygin.Y,Malin.B," Anonymization of longitudinal electronic medical records",published in information technology in Biomedicine (volume:16,issue:3), 2012.
[13] Poulis.G, Skiadopoulos.S, Loukides.G,Gkoulalas-divanis.A," Distance-based k^m-anonymization of trajectory data", PUBLISHED IN 14TH International conference on mobile data management,2013.
[14] Burke.M.J, Kayem.A.V.D.M," k-anomity for privacy preserving crime data publishing in resource constrained environments," published in international conference on advanced information networking and application workshop,2014.
[15] Ningui Li, Tiancheng Li and Suresh Venkatasubramanian " Closeness: A new privacy measurefor data publishing", IEEE Transactions on Secure and Dependable Computing, July 2010.
[16] N. Li, T.Li, and S.Venkatsubramanian,"t-closeness : privacy beyond k-anonymity and l-diversity", Proceedings of ICDE pp.106-115,2007.
[17] N. Li, and T.Li, "Injector: Mining background knowledge for data anonymization", Proceedings of ICDE,2008.
[18] A.Machanavajjhala, J.Gehrke, D.Kifer and S.Venkatasubramaniam" l-diversity: privacy beyond k-anonymity", Proceedings of ICDE,p.24,2006.
[19] K. LeFeVer, D.DeWitt and R.Ramakrishnan ," Mondrian Multidimensional K-anonymity", Proceedings of .ICDE, p.25,2006.
[20] P.Samarati, "Protecting respondents privacy in microdata release",IEEE trans,pp1010-1027,dec.2001.
[21] L.Sweeney,"K-anonymity :A model for protecting privacy",pp.557-527, International Journal on Uncertainity, Fuzziness and Knowledge-based Systems, 10(5), 2002.
[22] Balamurugan Shanmugam, Visalakshi Palaniswami, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013
[23] Balamurugan Shanmugam, Visalakshi Palaniswami, R.Santhya, R.S.Venkatesh "Strategies for Privacy Preserving Publishing of Functionally Dependent Sensitive Data: A State-of-the-Art-Survey", Australian Journal of Basic and Applied Sciences, 8(15) September 2014.
[24] Charanyaa, S., et. al., , A Survey on Attack Prevention and Handling
Strategies in Graph Based Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 2(10): 5722-5728, 2013.
[25] Charanyaa, S., et. al., Certain Investigations on Approaches forProtecting Graph Privacy in Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 1(8): 5722-5728, 2013.
[26] Charanyaa, S., et. al., Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization. International Journal of Innovative Research in Computer and Communication Engineering, 2(3): 3554-3561, 2014.
[27] Charanyaa, S., et. al., , Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization. International Journal of Advanced Research in Computer and Communication Engineering, 3(2): 5722-5728, 2014.
[28] Charanyaa, S., et. al., Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[29] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Certain Investigations on Strategies for Protecting Medical Data in Cloud", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
[30] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Investigations on Remote Virtual Machine to Secure Lifetime PHR in Cloud ", International Journal of Innovative Research in Computer and Communication Engineering Vol 2, Issue 10, October 2014
[31] V.M.Prabhakaran, Prof.S.Balamurugan, S.Charanyaa," Privacy Preserving Personal Health Care Data in Cloud" , International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[32] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, "Investigations on Evolution of Strategies to Preserve Privacy of Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[33] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Certain Investigations on Securing Moving Data Objects" International Journal of Innovative Research in Computer and Communication Engineering, 2(2): 3033-3040, 2014.
[34] P.Andrew, J.Anish Kumar, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Survey on Approaches Developed for Preserving Privacy of Data Objects" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[35] S.Jeevitha, R.Santhya, Prof.S.Balamurugan, S.Charanyaa, " Privacy Preserving Personal Health Care Data in Cloud" International Advanced Research Journal in Science, Engineering and Technology Vol 1, Issue 2, October 2014
[36] S.Balamurugan, S.Charanyaa, "Principles of Social Network Data Security" LAP Verlag, Germany, ISBN: 978-3-659-61207-7, 2014.

BIOGRAPHIES

K.Deepika, P.Andrew 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.**