SECURITY PORTRAYAL AND EVALUATION IN INFORMATION DISTRIBUTING

[1]B.Shirisha, [2]Dr. R. Jegadeesan [3]P.Pranitha, [4]R.Saikumar, [5]D.Saikrishna, [6]JaveriaTaj

[1,4,5,6]Final year Student Computer science and Engineering, [2,3]Associate Professor-CSE

[1,2,3,4,5,6]Jyothishmathi Institute of Technology and Science, Karimnagar, India

Abstract: The growing ability to track and acquire huge amounts of records with the use of current hardware technology now has lead to an activity in the improvement of facts mining algorithms which keep consumer privacy. A recently proposed method addresses the difficulty of privateness upkeep by means of perturbing the records and reconstructing distributions at an aggregate stage in order to perform the mining. Perturbing data is capable to preserve privacy whilst gaining access to the information implicit in the authentic attributes, distribution reconstruction process naturally leads to some loss of information which is appropriate in many practical situations. To manage these concerns, numerous Privacy-Preserving Data Publishing (PPDP) methods have been proposed in literature but they, lack a proper security portrayal and estimation. It initially presents a novel multi-variable privacy, portrayal and evaluation model. In light of this model, by investigating the earlier and back adversarial belief about quality estimations of individuals. The analysis will break down the affectability of any identifier in security portrayal.

At that point, the privacy should not be estimated depending on one measurement. It may lead to security misinterpretation .By the utilization of two different measurements for analysis of protection spillage, distribution spillage, and entropy spillage. Utilizing these measurements, the foremost notable PPDP systems are, for example, k-anonymity, l-diversity, and t-closeness. In view of the structure and the proposed measurements, the discovery of all the current PPDP plans has constraints in security portrayal. The proposed security portrayal and estimation structure adds to better understanding and assessment of those procedures. Thus, it provides an establishment to plan and investigation of PPDP plans.

Index Terms: *perturbing data, security portrayal, protection spillage*

I. INTRODUCTION

For the medical analysis, marketing research and economical measures data sets are considered a valuable source of information. These datasets will embrace information regarding people that contain social, medical, statistical, and client information. Several organizations, firms and institutions publish privacy connected datasets and the shared dataset offers helpful social information to researchers, it also creates privacy considerations and security risks to the people whose information square measure within the table. To avoid identification of individuals from records in advertised data, unambiguously identifying information like names and Social Security numbers are evacuated from the table. whereas the apparent personal identifiers detached from the table, the quasi-identifiers like zip-code, age, gender may still be used to uniquely identify a significant portion of the population since the released data makes it possible to infer or limit the available options of individuals than would be possible without releasing the table.

The deluge incidents of privacy associated to spurred an extended line of analysis in privacy notions for knowledge business and analysis, such as k-anonymity-diversity and t-closeness, to name many. A table satisfies k-anonymity if every quasi-identifier attribute within the table is indistinguishable from a minimum of k-1 other quasi-identifier attributes; such a table is termed as k-anonymous table. As long as k-anonymity protects identity disclosure of individuals by linking attacks, it's skimpy to stop attribute disclosure with facet information. Facet information is combined with released data it makes available to infer the possible sensitive attributes adore a private. Once the correspondence between the symbol and also the sensitive attributes is discovered for a private, it may harm the individual and also the distribution of the whole table. To alter this issue, l-diversity was introduced in L-diversity needs sensitive attributes contain atleast well-represented values in every equivalence category. As stated in l-diversity has 2major issues. One, is that it limits the adversarial information, whereas it's potential to acquire information of a sensitive attribute from usually available international distribution of the attribute. Another problem is that each one attributes area unit assumed to be categorical, which assumes that the opponent either gets all the information or gets nothing for a sensitive attribute.

In the authors propose a privacy notion known as t-closeness. They 1st formalize the concept of world background knowledge and propose the bottom model t-closeness. This model requires the distribution of a sensitive attribute in any equivalence category to be near to the distribution of the attribute in the overall table (i.e., the gap between the 2 distributions ought to be no over a threshold

This distance was introduced to live the data gain between the posterior belief and previous belief through the Earth Mover Distance (EMD) metric, that is depicted because the information gain for a particular individual over the complete population is associate in Nursing abstract distance between two distributions that doesn't have any intuitive relation with privacy discharge. Moreover, The tendency to show during this paper, the distance between two distributions cannot be simply quantified by one mensuration. T-closeness conjointly has many limitations that may be represented later. The state of the art PPDP techniques are going to be analyzed.

Research on knowledge privacy has been centered on privacy definitions, such as k-anonymity, l-diversity, and t-closeness. whereas these models solely take into account minimizing the amount of privacy leak while not directly mensuration what the somebody might learn, there's a motivation to search out consistent measurements of what quantity information is leaked to associate degree somebody by commercial enterprise a dataset.

In this paper,start by introducing our novel information publication framework. The planned framework consists of two steps. First, This tend to model attributes in a very dataset as a multi variable model. supported this model, This tend to area unit able to re-define the previous and posterior adversarial belief regarding attribute values of people. Then this tend to characterize privacy of those people supported the privacy risks hooked up with combining totally different attributes. This model is a additional precise model to explain privacy risk of publication datasets.

For a given dataset, before it's discharged, To work out to what extent this will reach privacy. Therefore, The tendency to introduce a brand new set of privacy quantification metrics to live the gap between previous information belief associate degreed posterior information belief of an human, from each native and international views. Specifically, Tendency to introduce two privacy leakage measurements: distribution leakage and entropy leakage. This discuss and explanation the two measurements and illustrate examples. This tend to show however considering only one metric ignoring the result of the opposite powerfully contributes to the data outpouring and successively affects the privacy. An intuitive example for this drawback is reviewing a blood work. A medical practitioner needs to review the relation between mixtures of all measures within the blood work. This tend to show that a reduced distribution run between sensitive attribute values distributions of the initial and therefore the printed datasets doesn't primarily reach the minimum entropy run that associate someone might gain. In fact, It show that distribution and entropy run square measure two completely different measures. This tend to believe that for a printed dataset to achieve higher privacy, each metrics have been taken as consideration.

II. RELATED WORK

Verykios et al [1] Privacy renovation techniques are an essential answer strategy because one-of-a-kind methods can be used to regulate data, such as heuristics, cryptography, and randomization. proved that until total queries have been sub-linear in database size, a large quantity of noise was required to keep away from a breach, making the database almost useless. A databases come to be larger, probabilities of being capable to query a sub-linear number of instances is realistic. Dwork &Nissim [2] in addition investigated this situation, generalizing beforehand work in 2 essential directions: multi-attribute databases (earlier work dealt solely with single-attribute databases) and vertically partitioned databases, where extraordinary attributes subsets are saved in exceptional databases. Clifton et al [3] suggested that a answer to this was a aspects toolkit that can be combined for particular privacy-preserving data mining applications. They additionally presented aspects of such a toolkit showing how they should be used to resolve many privacy preserving records mining problems. New tools for building PPDM techniques had been developed and validated new functions for this technology. There are still many challenges in this area, such as defining privacy constraints. As an instance of the doable difficulties, think about a situation where the data mining effects violate privacy. Secure multiparty computation definitions do not resolve the problem. R. Agrawal [4] PPDM, the concrete case of constructing a decision-tree classifier from trending information in which the values of man or woman documents have been perturbed. The ensuing data information seem very different from the unique data and the distribution of facts values is also very extraordinary from the unique distribution. While it is not possible to precisely estimate unique values in character information records, This advise a-novel reconstruction system to accurately estimate the distribution of unique data values. By the usage of these reconstructed distributions, This can build classifiers whose accuracy is same to the accuracy of classifiers built with the unique data. J. Traub [5] The techniques used for preventing statistical database compromise fall into two categories: noise addition, where all information and/or facts are available but are only approximate as an alternative than exact, and restriction, where the gadget only provides those information and/or data that are considered safe. In either case, a technique is evaluated with the aid of measuring each the records loss and the done degree of privacy. The goal of statistical records protection is to maximize the privateness whilst minimizing the facts loss. In order to consider a unique technique it is necessary to set up a theoretical decrease bound on the facts loss crucial to obtain a given level of privacy. In this chapter, author existing an overview of the hassle and the most important outcomes in the area. K. Wang [6] A realistic and efficient algorithm for figuring out a generalized model of records that masks touchy records and remains useful for modelling classification. The generalization of data is applied via specializing or detailing the stage of information until a minimum privateness requirement is violated. This top-down specialization is herbal and efficient for handling both express and continuous attributes. While generalization can also cast off some structures, different structure emerge to help. Our consequences show that exceptional of classification can be preserved even for fairly restrictive privateness requirements. This work has incredible applicability to both public and personal sectors that share statistics for mutual advantages and productivity. Bertino et al [7] Reviewed and summarized current standards and metrics in evaluating privacy retaining techniques. He aim of PPDM algorithms is to extract relevant expertise from massive statistics whilst protecting sensitive information .An thing in diagram of such algorithms is identification of assessment criteria and associated benchmarks development. Recent research devoted effort to determine a trade-off between proper to privacy and need of knowledge discovery. Often no privatness retaining algorithm exists that can outperform all others on all criteria. Hence, it is quintessential to make sure a comprehensive view on metrics associated to current privacy preserving algorithms to gain insights on how to diagram higher measurement and PPDM algorithms. Oliveira et al [8] laid out what wishes to be finished and takes steps to suggest such standardization: First, describe problems in defining which data is personal in facts mining ,and discuss how statistics mining violates privacy. Then, based on users' personal information and data regarding their collective activity, the privacy preservation in records mining is defined. Second, analyze implications of Organization for Economic Cooperation and Development (OECD) data privacy principles in a data mining context and suggest PPDM policies based on such principles. Finally, advocate requirements to guide development/deployment of technical solutions. Yang et al [9] confirmed that many information mining algorithms can be decreased to 3 fundamental operations, impenetrable implementation on which – Secure Product of Summations (SPoS), Secure Ratios of Summations (SRoS), and Secure Comparison of Summations (SCoS) – lead to privacy retaining statistics mining solutions. The authors show that previously privacy retaining facts mining solutions are unsatisfactory due to participant’s collusion and hence provided new implementation of such operations designed to preserve collusion. L. Sweeney [10] A release provides k-anonymity safety if the information for each person contained in the release cannot be amazing from at least k-1 persons whose records additionally appears in the release. The k-anonymity safety model is necessary because it varieties the foundation on which the real-world structures recognized as Data fly, μ-

Argus and k-Similar furnish ensures of privateness protection. Campan [11] The proposed method consists of specifying quasi identifiers' generalization constraints, and accomplishing p-sensitive k-anonymity within the imposed constraints. It's thought that limiting the quantity of allowed generalization when overlaying micro data is integral for real life datasets and applications. The two limited p-sensitive k-anonymity model was once added and an algorithm for generating limited p-sensitive k-anonymous micro data was presented. Navarro-Arribas [12] presented the anonymization of query logs the usage of micro aggregation. The notion ensures the k-anonymity of the customers in the query log, while preserving its utility. It provided the evaluation of the inspiration in real query logs, confirmed the privateness and utility achieved, as well as providing estimations for the use of such data in information mining methods primarily based on clustering. Atzori et al [13] studied when statistics mining effects disclosure represents, per a chance to people anonymity recorded in analyzed database. The proposed approach's novelty is that it focuses on privacy patterns compliance objective definition without reference to preconceived knowledge of what is sensitive, primarily based on as an alternative intuitive and realistic constraint that humans anonymity be guaranteed. Specifically, the problem addressed arises from possibilities of inferring from regular object set mining output (set of item-sets with support larger than a threshold), patterns existence with low assist (smaller than anonymity threshold k). The new work developed a easy methodology to block inference opportunities by introducing distortion on dangerous patterns. Kenig et al [14] introduced a realistic approximation algorithm that allows solving the k-anonymization problem with an approximation warranty of O (ln k).The proposed algorithm achieves decrease facts losses than the leading approximation algorithm, as well as the leading heuristic algorithms. Friedman et al [15] prolonged k-anonymity definitions the use of them to show that a statistics mining mannequin does no longer violate folks k-anonymity represented in learning examples. The proposed extension affords a tool to measures anonymity retained when data mining. The proposed mannequin can be applied to various information mining issues like classification, clustering and association rule mining. Singh et al [16] proposed a method for extended grouping of records units which provide PPDM the usage of ID3 algorithm with k-mean clustering algorithm on randomization response technique. It concludes that the accuracy of the prolonged group can be increase if it can classify the bounding restrict of the information set the usage of Genetic algorithm supported by k- mean. The proposed work is to check out the accuracy level of the dataset if the clusters are divided into internal clusters so that their privateness can be improved. Sumana & Hareesh et al [17] analyzed various anonymization techniques in PPDM used for preserving privacy of the data. The main goal of anonymization was to secure access to the sensitive information and at the same time providing aggregate information to the public. Confidential information revealing could be linked to the individuals, so the task was a challenging one. Mazleena Salleh [18] The contemporary privateness maintaining facts mining methods are labeled primarily based on distortion, association rule, conceal association rule, taxonomy, clustering, associative classification, outsourced data mining, distributed, and k-anonymity, the place their top notch blessings and disadvantages are emphasized. This cautious scrutiny displays the past development, present research challenges, future trends, the gaps and weaknesses. Further considerable enhancements for greater sturdy privacy protection and protection are affirmed to be mandatory. A.

Machanavajjhala [19] In recent years, a new definition of privacy called k-anonymity has gained popularity. In a k-anonymized dataset, each record is indistinguishable from at least k - 1 other records with respect to certain identifying attributes. S. Venkatasubramanian [20] Recently, countless authors have recognized that k-anonymity cannot stop attribute disclosure. The thought of l-diversity has been proposed to tackle this; l-diversity requires that each equivalence category has at least l well-represented values for each touchy attribute. In this paper there exhibit that l-diversity has a variety of limitations. In particular, it is neither imperative nor enough to prevent attribute disclosure. It suggest a novel privateness notion referred to as t-closeness, which requires that the distribution of a sensitive attribute in any equivalence type is shut to the distribution of the attribute in the ordinary table (i.e., the distance between the two distributions ought to be no extra than a threshold t). Here instance is showing to use the Earth Mover Distance measure for our t-closeness requirement. X. Xiao [21] A new generalization framework based on the idea of personalized anonymity is presented. Our approach performs the minimal generalization for fulfilling everybody's requirements, and thus, retains the greatest quantity of facts from the microdata. This raise out a careful theoretical learn about that leads to valuable perception into the behavior of alternative solutions. In particular, our evaluation mathematically reveals the occasions the place the previous work fails to protect privacy, and establishes the superiority of the proposed solutions. D. Rebollo-Monedero [22] T-Closeness is a privateness mannequin recently defined for statistics anonymization. A information set is said to fulfill t-closeness if, for each crew of information sharing a combination of key attributes, the distance between the distribution of a private attribute in the team and the distribution of the attribute in the entire statistics set is no more than a threshold t. Here, it define a privateness measure in phrases of data theory, similar to t-closeness. Then, by way of the usage of the tools of that theory to exhibit that our privacy measure can be finished by using the submit randomization method (PRAM) for protecting in the discrete case, and through a structure of noise addition in the familiar case. Pingshui Wang1 [23] At current most privateness keeping algorithms primarily based on l-diversity mannequin are restricted solely to static records release. It is low effectivity and vulnerable to inference attack if these anonymous algorithms are at once applied to dynamic information publishing. To address this issue, this paper analyzes various inference channels that maybe exist between a couple of anonymized datasets and discusses how to avoid such inferences and offers an fantastic approach to securely anonymize a dynamic dataset based on incremental clustering: incremental l-diversity algorithm. Theory evaluation and experiment results exhibit that the proposed method is fine and efficient. K. Lefevre, [24] In this paper, writer provided a practical frame because of enforcing certain model concerning stability toughness permanency stability k-anonymization, called full-domain generalization and added a engage over algorithms for producing deficient full-domain generalizations, then show so much these algorithms function on to an rule about magnitude faster than previous algorithms concerning twins real-life databases. Besides full-domain generalization, severa sordid fashions have additionally been proposed for k-anonymization. The second performance within that paper is a individual taxonomy so much categorizes preceding models then introduces half promising instant alternatives. P. Samarati [25] address the trouble of releasing microdata while safeguarding the anonymity of the respondents to which the data refer. The strategy is primarily based on the definition of k-anonymity which illustrate how the k-anonymity can be supplied except compromising the integrity (or truthfulness) of the facts released by way of using generalization and suppression techniques. So, it introduces the concept of minimal generalization that captures the property of the release method not to distort the data extra than wanted to reap k-anonymity, and present an algorithm for the computation of such a generalization.This talk about possible desire insurance policies to choose amongst exceptional minimal generalizations.

III.EXISTING SYSTEM

A table fulfills k-anonymity if each record in the table is vague from at any rate k - 1 other record as for each arrangement of semi identifier traits; such a table is known as a k-anonymous table. The possibility of k-anonymity was proposed to battle record linkage assaults.

A table is said to have l-diversity if each proportionality class of the table has l-diversity. L-diversity speaks to a critical advance past k-anonymity in securing against characteristic linkage. Be that as it may, it is helpless to assaults, for example, skewness and comparability assaults.

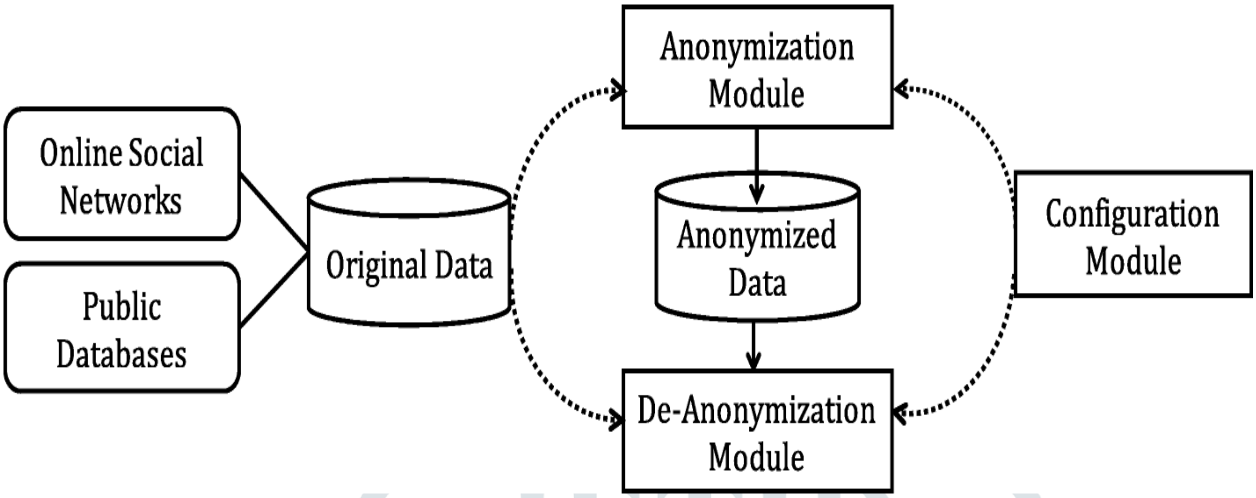
A table is said to have t-closeness if all proportionality classes have t-closeness. The separation utilized in this distributing strategy is the earth mover's separation. EMD is essentially the insignificant measure of work expected to change one conveyance to another by moving appropriation mass between every one of them.

IV.PROPOSED SYSTEM

In this paper, presenting our novel information distributing system. The proposed structure comprises of two stages:

1. To start with the demonstrate characteristics in a dataset as a multi-variable model. In view of this model, This can re-characterize the prior and posterior adversarial conviction about quality estimations of people.
2. At that point of portray protection of these people dependent on the security dangers joined with consolidating distinctive qualities. This model is to be sure a progressively exact model to portray protection danger of distributing datasets.

V.SYSTEM ARCHITECTURE



The distribution spillage and entropy spillages are two unique measurements.

Distribution spillage:

The distribution spillage could be seen as a proportion of the general difference of property estimations conveyance from one state to the next. By and large, any protection saving distributing procedure changes the first dataset into a lot of equivalence classes. Spillage is estimated between the first appropriation of sensitive attribute values in the first and the distributed dataset for each given equivalence class.

Entropy spillage:

Maximum entropy of characteristic qualities in the distributed dataset does not accomplish the most extreme security. The most extreme entropy compares to the uniform distribution of characteristic qualities. This sort of distribution can be ideal if the foundation data of a adversary is ignored. However, given that a adversary has some earlier belief about unique attribute values distribution, it is ideal to keep up a similar entropy level after distributing.

To justify this, let us expect the situation when the characteristic qualities distribution is a stage of the original distribution. unless if the original distribution is uniform, whatever the distribution spillage is, the entropy spillage will dependably be zero. Given the learning of the distribution of delicate property estimations of the original distribution, an adversary has a specific dimension of vulnerability about people trait esteems. Any adjustment in this dimension of vulnerability is viewed as a spillage. A goal of any information distributing method would limit this spillage. In the interim, This don't have the foggiest idea what number of measurements would be adequate to evaluate security. In any case, The trust that any further proposed free measurements that would add to achieving an ideal and provably adequate arrangement of measures, can be added to the proposed quantitative estimation system.

VI.CONCLUSION

In this paper, Extensive portrayal is presented and novel measurement techniques for security to manage the issue of protection evaluation in protection saving information distributing. So as to consider the security loss of consolidated properties, Information distributing as a multi-social model. The re-characterized the earlier and back convictions of the enemy. The proposed model and ill-disposed convictions add to a progressively exact security portrayal and evaluation. Bolstered by in sightful models, At that point demonstrated that protection couldn't be measured dependent on a solitary measurement. Two distinctive protection spillage measurements are proposed. In light of these measurements, the security spillage of any given PPDP strategy could be evaluated. Our tests exhibit how this could pick up a superior judgment of existing strategies and help examine their adequacy in achieving protection. Our work opens ways to a wide scope of research issues and questions including whether two measurements are adequate to assess security or there exist other free measurements that could help accomplish better protection evaluation. Another open issue is the streamlining of the first information speculation as to accomplish most extreme security dependent on our proposed measurements. Ordinarily, Trust that equality classes ought to be planned so that keeps both the entropy spillage and the distribution spillage underneath a specific foreordained dimension. This suggest us to think about a normal distributing situation. It likewise leave as an open issue for further research, enhancement of the picked set of semi identifiers with a target of limiting appropriation and entropy spillages inside the distributed table or explicit classes of higher security concerns.

VII.REFERENCES

[1] Verykios, Vasilios (2004)S.et al."State-of-the-art in privacy preserving data mining." .

[2] Jegadeesan,R., Sankar Ram,N. “Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling”, Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[3]Clifton C., Kantarcioglu M., Vaidya J., Lin X. & Zhu M.Y.(2002b).”Tools for PrivacyPreserving Distributed Data Mining”. ACM SIGKDDExplorations,Vol 4, No 2, pp. 28-34, ISSN 1931-0145.

[4]. R. Agrawal and R. Srikant, “Privacy-preserving data mining,” in Proc. 2000 ACM SIGMOD Int. Conf. Manag. Data (SIGMOD ’00). ACM, New York, NY, USA, 2000, pp. 439–450.

[5] Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 “A Recent Approach to Organise Structured Data in Mobile Environment” R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646.

[6]K. Wang, and P. S. Yu, “Top-down specialization for information and privacy preservation,” in Proc. 21st IEEE Int. Conf. Data Eng., 2005, pp. 205–216.

[7] Bertino, " A framework for evaluating privacy preserving data mining algorithms". Data Mining and Knowledge Discovery 11(2),121–154 (2005).

[8] Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[9] Yang, et al. "Collusion-resistant privacy-preserving data mining."Proceedings of the 16th ACM SIGKDD international conference on Knowl.

edge discovery and data mining. ACM, 2010.

[10] L. Sweeney, "k-anonymity: A model for protecting privacy," Int. J. Uncertainty, Fuzziness Knowl.-Based Syst., vol. 10, no. 5, pp. 557– 570, 2002.

[11]Campan(2010)"User-Controlled Generalization Boundaries for P-Sensitive K-Anonymity".In Proceedings of the ACM Symposium on Applied Computing (SAC2010).

[12] Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[13] M. Atzori (2005 "k-anonymous patterns".In Proceedings of the PKDD'05.

[14] B Kenig, T TassaA practical approximation algorithm for optimal k-anonymity Data Mining and Knowledge Discovery, 2012.

[15] A. Friedman, A. Schuster, R. Wolff, "Providing k-anonymity in data mining", VLDB 17 (4) (2008) 789–804.

[16] Singh, Soniya & Priyanka Gupta, "Comparative Study ID3 and C4.5 Decision Tree Algorithm: A Survey", International Journal of Advanced Information Science and Technology (IJAIST) Vol.27, No.27

[17]Sumana M, Hareesh K.S. and Shashidhara H.S., "An Approach of Private Classification on Vertically Partitioned Data", in the proceedings of International Conference and Workshop on Emerging Trends in Technology(ICWET 2010), February 26-27, ACM 2010.

[18]Yousra Abdul Alsahib S. Aldeen, MazleenaSalleh, and Mohammad AbdurRazzaque."A comprehensive review on privacy preserving data mining".

[19]Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1

[20] Dwork&Nissim 2004 "privacy preserving in data minig in vertically partitioned database". In crypto 2004,vol 3152 pp.528 ,544.

[21] Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[22] Oliveira et al 2004 “Towards standardization in privacy preservation in data mining”. In ACM SIGKDD 3rd Workshop on Data Mining standards,pp 7-17.

[23] Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 “NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD” Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[24] Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 “SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups“ Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[25] Jegadeesan,R.,SankarRam,T.Karpagam March-2014 “Defending wireless network using Randomized Routing process” International Journal of Emerging Research in management and Technology

[26] Navarro-Arribas, et al (2012) presented” The anonymization of query logs using micro aggregation”.

[27] Jegadeesan,R., Sankar Ram “Defending Wireless Sensor Network using Randomized Routing ”International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[28] J. Traub, Y. Yemini, and H. Wozniakowski, “The statistical security of a statistical database,” ACM Trans. Database Syst., vol. 9, pp. 672–679, 1984

[29] Jegadeesan,R., Sankar Ram , and J.Abirmi “Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy“ International journal of Advanced Research trends in Engineering.