iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2134

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Dynamic Privacy Pricing For Timely Rewards

Shatabdi Nandi[1], R. B. Sarooraj[2]
[1]*Department of Computer Science SRM University, Chennai*
[2]*Assistant Professor Department of Computer Science SRM University, Chennai*

Abstract
Aims: The Data Mining Technologies are growing day by day and becoming more popular. In this scenario, protecting individual's sensitive information is becoming a serious threat. There is another issue which is seeking much attention is, the exploitation of the value of personal data. Setting a price for individual's privacy is one form to conquer these threats is a measure though it is a tough issue. Different measures are taken to estimate the price, to estimate the rewards in several contexts and to set the price.
Results: By this paper, different policies have come across to carry out the above said strategies. Conclusion- It is useful to protect individual's privacy and to set the proper pay off.

I. INTRODUCTION

In current scenario, the value of personal data is becoming a major issue in 'Big Data' world. The security issues of anyone's privacy is jeopardized if any unauthorized party access it or that data is used for any improper use. In recent years one of the most important issues is to deal between exploiting the value of personal data and protecting individual's privacy [1]. Already different solutions have been proposed to realize Privacy Preserving Data Publishing (PPDP) [2] or Privacy Preserving Data Mining (PPDM) [3]. On the other hand, selling personal data on markets is a good solution for the privacy-concerned people and adding a boost into it, the economic analysis of privacy [4] is receiving much attention. The monetary value of privacy is highly dependent on the individuals as different persons have different views on their sensitive information and how the sensitive information is going to be used. In this paper , we see that multiple data owners are interacted sequentially by the Data collector and the price is set. Similar to some previous work [5] [6], the online echanism is adopted. Posted-price m

II. RELATED WORKS

Many researches have been done for preserving the privacy as well as different policies have been taken to get the pricing strategy . Still there are many fields where improvisations are needed on the existing solutions to develop a new and better solution.

A. Preserving the Privacy in Data Mining

The privacy-preservation can be done by using the following ways:

1) Two different parties that own their confidential databases, running on a Data mining algorithm without giving any unnecessary information to each other.
2) Privacy preserving data mining (PPDM) [3] techniques that tend to transform the original data that maintains the privacy constraints and set the result accordingly.
3) Optimization algorithm, known as k-anonymization. [7]
4) k^w –structured diversity anonymity [8], where k is an appreciated privacy and w is a time period, to monitor victim and together the attack knowledge.
5) Data suppression technique [9], which represents the privacy breach that also keeps the posted data accurate as much as possible.
6) Heuristic Algorithm named DSRRC (Decrease Support of R.H.S. item of Rule Clusters) [10] , which ensures the data quality while providing privacy for sensitive rules.
7) Using the 'impact factor' [11] which hides several rules and which modifies fewer ran sections.
8) Mechanisms that incentivizes the individuals to report their preferences according to different payment schemes.

B. Other Related Works

Incentive Compatible privacy-Preserving Data Analysis [12] to design incentive compatible privacy-preserving data analysis techniques. It is seen that different competing parties have different incentives. The participating parties must be prevented from

modifying their private input data. Current PPDA (Privacy Preserving Distributed Data Analysis) techniques cannot prevent this, until proper incentives are set. The Proposed system analyzes tasks based on some key theorems which tells the best choice for Any participating party. A Novel Privacy Decision Tree Induction [13]: Generally, Data Mining Algorithms have to extract knowledge from very large data sets. These data are to be shared among multiple users and in this case security is an important factor. In this paper a new system has been proposed which deals with an efficient privacy preserving decision tree induction algorithm that reduces the communication and computational cost.

C. Background

The works that are proposed in the previous sections are having several shortfalls. This section will give a brief background about the new approach proposed in this paper.

D. Idea Behind

The value of private data is growing increasingly and the security of individual's privacy is becoming an important issue now-a-days. New and efficient Data Mining techniques have attracted much attention in the past years, probably because of the 'Big Data' concept. Many researchers have proposed several policies to security of private data and to avoid the unwanted disclosure of sensitive information. In personal data market, the value of private information is an important task to calculate. To get the maximum payoff, the data collector dynamically adjusts the prices offered to the owners.

III. PROPOPSED WORK

Two learning policies have been proposed based on the Upper Confidence Bound. The former policy deals with the estimated price of the expected reward of a price by counting how many times the reward has been accepted by the data owner. The former policy treats with the time-variant data values.

A. Privacy Pricing

Each Data Owner owns their data and these data are collected by the Data Collector who pays the Data Owner against their sensitive information. Let , p be the price that the collector is willing to pay for one data record. The privacy attitude of the data owner is denoted by ɵ. A large ɵ indicates that the data owner is much concerned about his data. The corresponding probability density function is denoted by f (ɵ).

B. Bandit Formulation

A Bandit problem is usually formalized to design a learning policy to solve the exploitation-exploration trade-off.

C. Arms With Time-Variant Rewards

The stochastic bandit problem has an implicit assumption that each arm is associated with a time-invariant distribution reward, so the best arm remains unchanged over time. But, this assumption actually does not work. Before making use of the collected data records, the collector performs data anonymization to protect data owners' privacy.

D. Learning Policy

1) *Upper Confidence Bound:* The learning policy UCB1 proposed in [14] and its variants are widely applied to bandit problems. The basic idea of UCB1 is to estimate the unknown expected reward of each arm by making a linear combination of previously observed rewards of the arm.

E. Estimiting Cummulative Distribution-

A new approach has been proposed to modify the policy UCB to make a more accurate estimate of the expected reward.

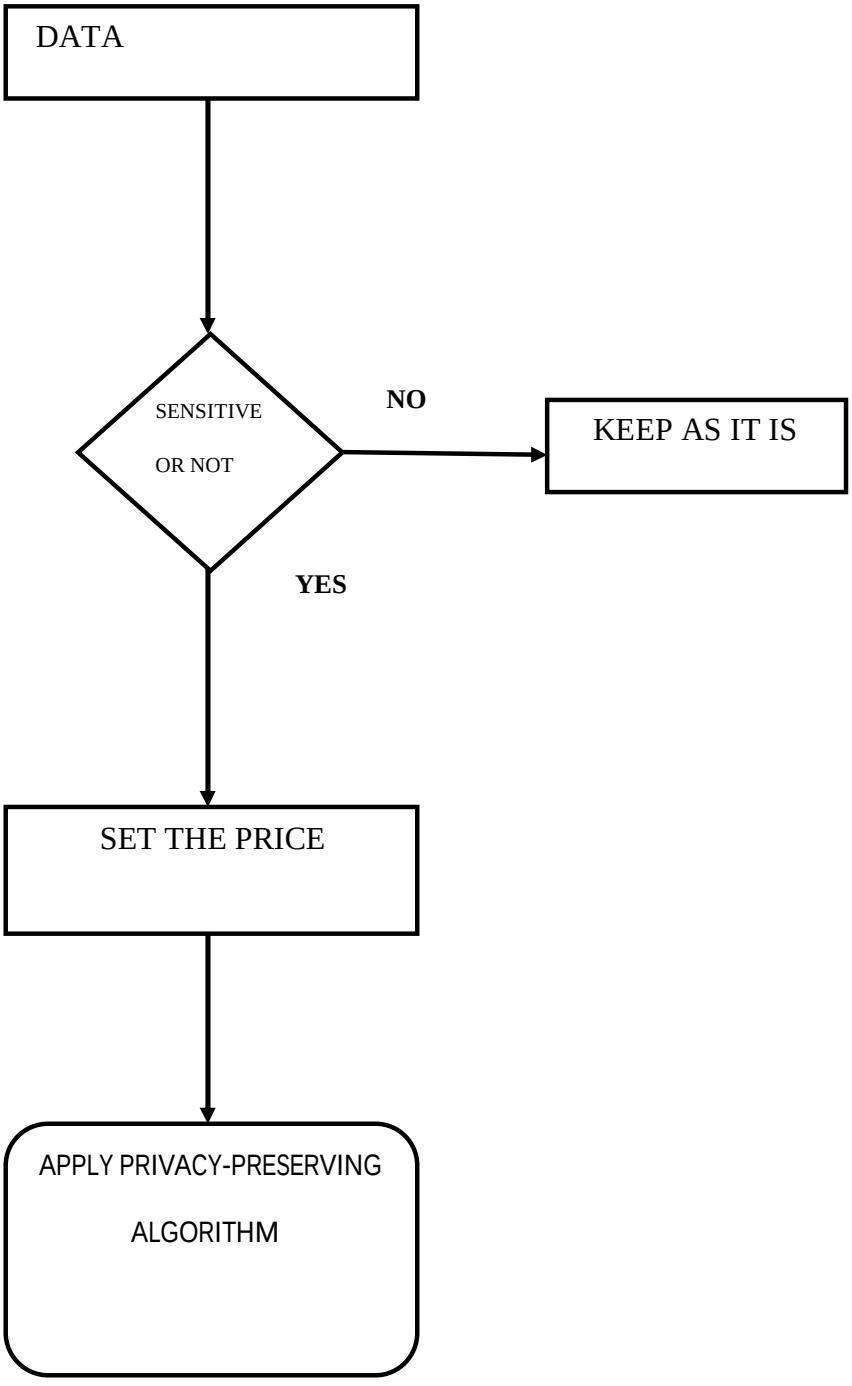
F. Contextual Bandit Approach

Instead of estimating the cumulative distribution, here we view the time-variant characteristic of the bandit problem from a different perspective.

G. Flow Diagram

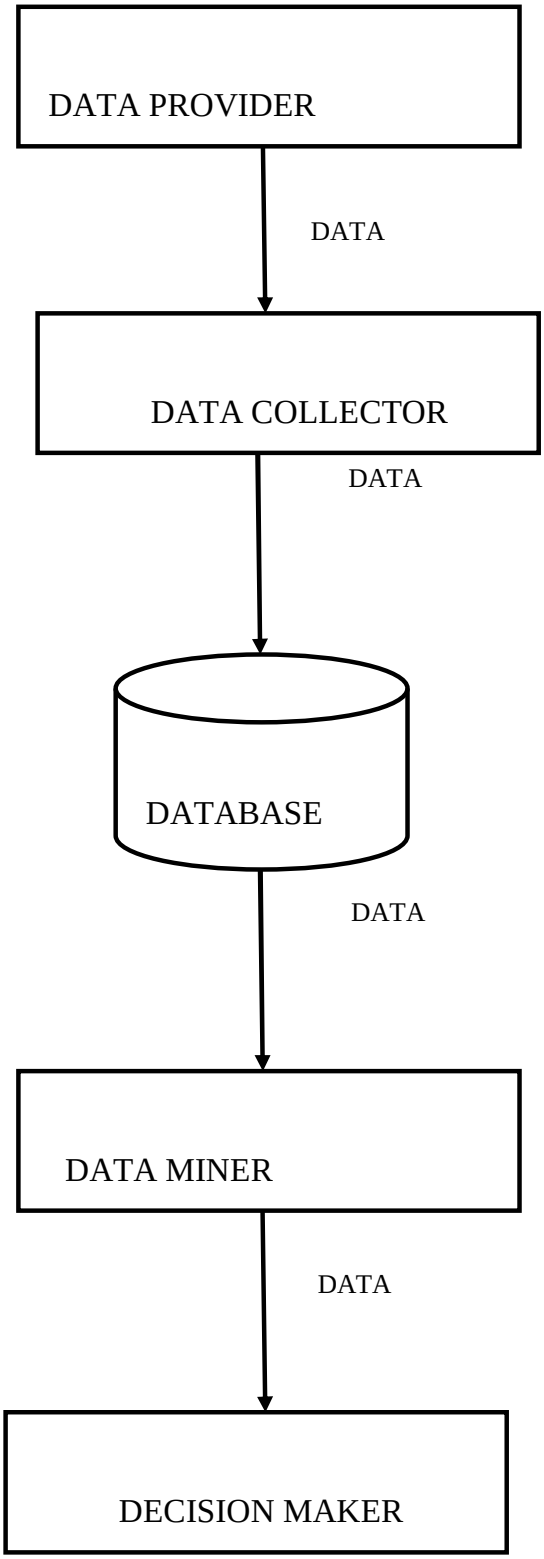
1) *Data Flow-*
2)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

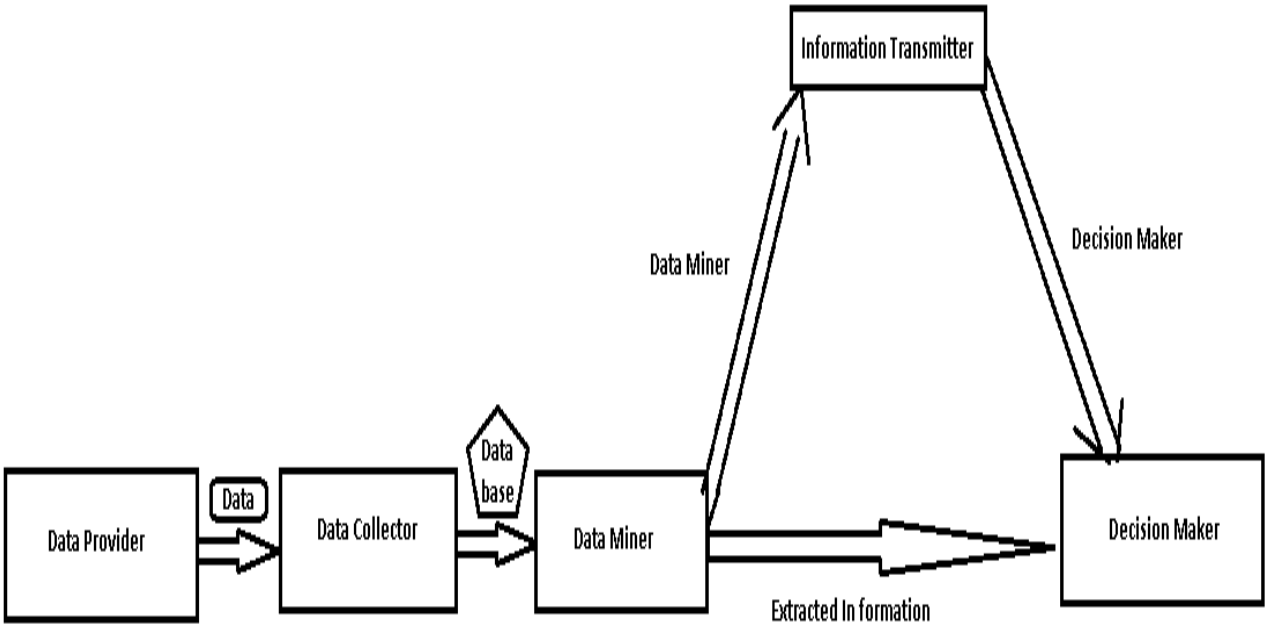


ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

H. System Flow



I. System Architecture



IV. CONCLUSION

The proposed system formulates the pricing problem as a multi-armed bandit problem in an enhanced and efficient manner. The distribution of the arms is formulated as time-variant.

A. Conflict of Interest

Author declares no conflict of interest.

V. ACKNOWLEDGEMENT

The author gratefully acknowledge the technical support given by Mr. R. B. Sarooraj, Assistant Professor, Dept. of Computer Science and Engineering ,SRM University, Chennai.

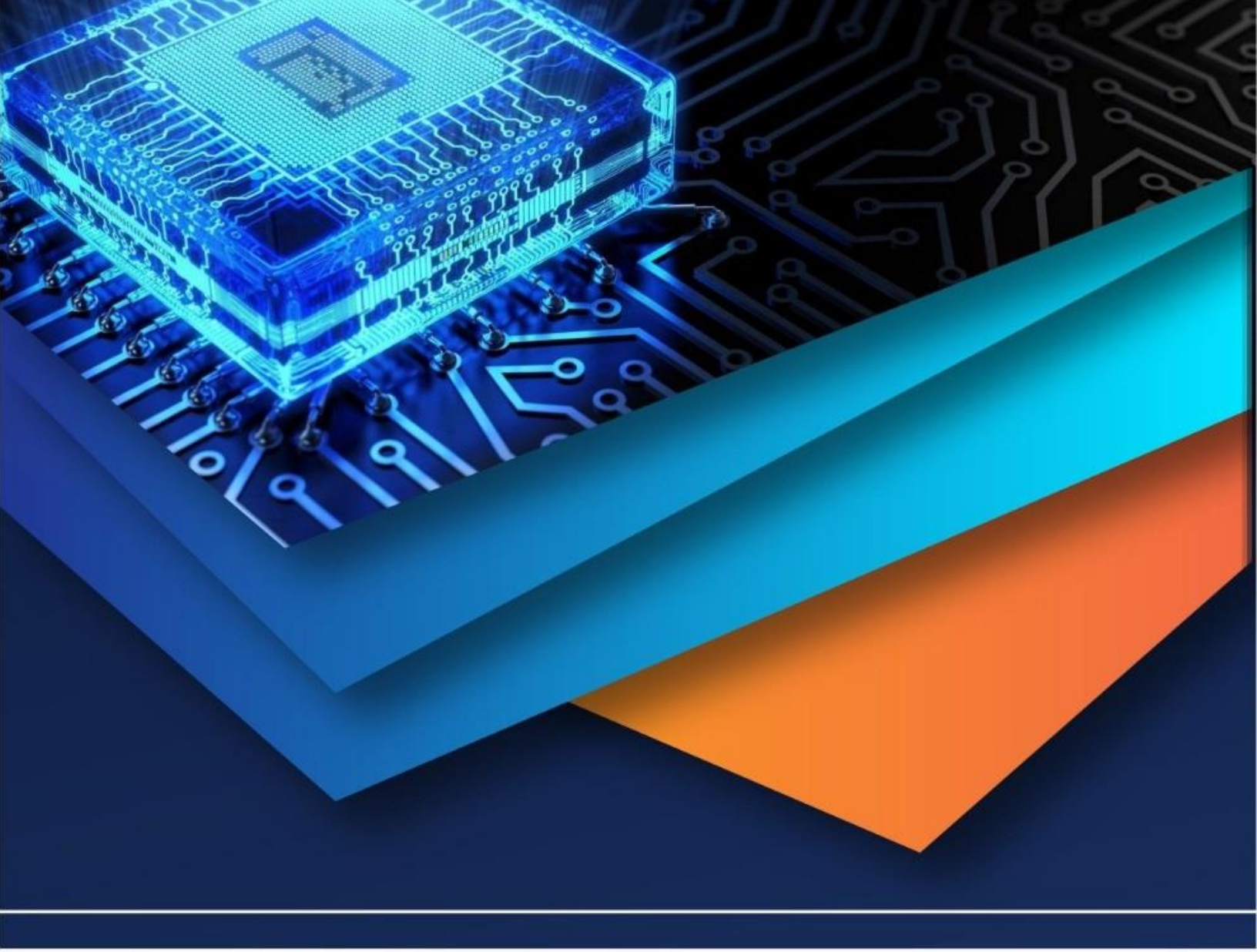
A. Financial disclosure

No financial support was received to carry out this project.

REFERENCES

[1] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, “A framework for categorizing and applying privacy-preservation techniques in big data mining,” Computer, vol. 49, no. 2, pp. 54–62, Feb. 2016.
[2] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, “Privacy-preserving data publishing: A survey of recent developments,” ACM Comput. Surv., vol. 42, no. 4, pp. 14:1–14:53, Jun. 2010.
[3] R. Agrawal and R. Srikant, “Privacy-preserving data mining,” SIGMOD Rec., vol. 29, no. 2, pp. 439–450, Jun. 2000.
[4] A. Acquisti, C. R. Taylor, and L. Wagman. (Mar. 2015). The Economics of Privacy. [Online]. Available: http://ssrn.com/abstract=2580411
[5] A. Singla and A. Krause, “Truthful incentives in crowdsourcing tasks using regret minimization mechanisms,” in Proc. 22nd Int. Conf. WorldWide Web, 2013, pp. 1167–1178
[6] K. Amin, A. Rostamizadeh, and U. Syed, “Learning prices for repeated auctions with strategic buyers,” in Proc. Adv. Neural Inf. Process. Syst., 2013, pp. 1169–1177.
[7] R. J. Bayardo and R. Agrawal, ``Data privacy through optimal k-anonymization," in Proc. 21st Int. Conf. Data Eng. (ICDE), Apr. 2005, pp. 217_228

[8] C.-H. Tai, P.-J. Tseng, P. S. Yu, and M.-S. Chen, ``Identity protection in sequential releases of dynamic networks," IEEE Trans. Knowl. Data Eng., vol. 26, no. 3, pp. 635_651, Mar. 2014.
[9] M. Terrovitis and N. Mamoulis, ``Privacy preservation in the publication of trajectories," in Proc. 9th Int. Conf. Mobile Data Manage. (MDM), 2008, pp. 65_72
[10] C. N. Modi, U. P. Rao, and D. R. Patel, ``Maintaining privacy and data quality in privacy preserving association rule mining," in Proc. Int. Conf.Comput. Commun. Netw. Technol. (ICCCNT), Jul. 2010, pp. 1_6.
[11] K. Pathak, N. S. Chaudhari, and A. Tiwari, ``Privacy preserving association rule mining by introducing concept of impact factor," in Proc. 7thIEEE Conf. Ind. Electron. Appl. (ICIEA), Jul. 2012, pp. 1458_1461.
[12] R. Nix and M. Kantarciouglu, ``Incentive compatible privacy-preserving distributed classification," IEEE Trans. Dependable Secure Comput., vol. 9, no. 4, pp. 451_462, Jul. ,1
[13] M. A. Sheela and K. Vijayalakshmi, ``A novel privacy preserving decision tree induction," in Proc. IEEE Conf. Inf. Commun.Technol. (ICT), Apr. 2013, pp. 1075_1079.
[14] P. Auer, N. Cesa-Bianchi, and P. Fischer, “Finite-time analysis of the multiarmedbandit problem,” Mach. Learn., vol. 47, nos. 2–3, pp. 235–256, 2002.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY