International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Association Rule hiding Using Grey Wolf Optimization Algorithm

S. Sharmila, S.Vijayarani

Abstract**: *Data mining of Privacy-preserving is another research field that way to ensure private data and ignore the spillage of data on the methodology of data mining. The objective of this examination is to secure individual data and to anticipate the introduction of this information during the data mining process. There are distinctive strategies in privacy data mining field. One of the strategies is association rule mining (ARM). The essential motivation behind ARM is to conceal sensitive association rules. PPARM is an imperative methodology in this field which hides the sensitive association rules. The algorithms of wide range have been made to hide delicate records. In this work, a new and powerful methodology has been shown for touchy data stowing away. GWO algorithm was proposed, in this algorithm data, contortion procedure was used to conceal the sensitive association rules. Fitness functions are used to accomplish the solution with the least indications. Likewise, the runtime has been decreased and provided better protection of data quality. The proposed technique's efficiency was assessed by directing a few trials on various databases. The performance results of the proposed algorithms and two other existing algorithms on various database shows that the GWO Algorithm has higher efficiency contrasted to various algorithms.***

Index Terms**: *Data mining, Grey Wolf Optimization (GWO), Privacy Preserving Association Rule Mining (PPARM), Sensitive Data Hiding, Privacy Preserving Data Mining (PPDM)***

I. INTRODUCTION

Data mining is the technique of evaluating lot of information to find sensitive data and patterns. The process of data mining is utilized with a plenty of information in the organizations and business relationship to allow it to settle on reasonable options [1]. Expansive data supplies include delicate data which must be verified over unapproved access. Ensuring the privacy of these data is a vital objective for the research group of government associations and database security. Henceforth, the primary problem is to make a balance among the privacy of data and the client's demands. The organizations which keep up this database are stressed over the significance of such a colossal exchange of database. The patterns of hidden knowledge could give understanding into the data owners just as being expensive in essential strategic planning and decision making. In some cases, associations are keen on working together with their datasets with associations of comparable domains to examine their databases for collective advantages [12].

For instance, some hospitals need to share the information of diagnosis of their patients to process inquire without uncovering the information to one another or third parties. Many banks need to provide the special standard in the policy of credit card and would prefer not to release the information of their client to different banks. At that point, they need a method that could analyze their information on keeping up the data privacy [15].With the development of computer's data storage capacity, they proposed an assortment of new data mining algorithms. The utilization of data mining methods may imperil the database holder's security [22]. Hence, another research subject called PPDM was proposed. As of late, PPDM has turned into a critical issue as a result of the extensive measure of individual data utilized by numerous organizations. Most of the times, clients are hesitant to uncover their own information except if the privacy of their delicate data is ensured [2]. To keep the exposure of sensitive data, in this research the algorithms make few certain improvements in the database and adjust measures of information in the database. In any case, modifying and deforming the database in terms to secure the secrecy of sensitive data is not impeccable and has few drawbacks [23].

PPDM mostly considers two parameters. First, how to ensure that the information, for example, name, number of ID card, address, etc. does not uncover in the data application process. Sensitive real information is whether reconsidered or removed from the first database. Reason for doing this is to secure individual protection against vulnerable information. Second is how to make applications with more advantages [13]. The service data excavation algorithm has sensitive knowledge to uncover the database which conceivably damages the data protection, hence, should evacuate the sensitive standard. Mining valuable sensitive records utilizing data mining technique from the database may eliminate few information [17].

Association rules are an imperative strategy for finding patterns hidden in raw information and it is the important vital technique created and broadly examined by databases and network of data mining. Association mining discovers its uses over numerous fields [14]. One of popular uses of ARM is in the business domain where the revelation of procurement practices or connections among productions is helpful for making decisions and creating a compelling trading technique. Notwithstanding, over the most recent years, there's been a critical advancement in the field of ARM [18].

The paper has the sections following: Section 2 contains literature survey of background and related work. Section 3 represents the problem statement of the proposed research. Section 4 contains explanation of proposed optimization algorithms.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)

S. Sharmila, Ph.D in Department of Computer Science, Bharathiar University, Coimbatore, and Tamilnadu, India.

S.Vijayarani, Assistant Professor of Department of Computer Science at Bharathiar University, Coimbatore, India.

In section 5, description of performance evaluation and dataset is presented. Section 6 is about experimental results. Section 7 contains conclusion.

II. BACKGROUND AND RELATED WORK

Verykios et al. proposed five algorithms. In these, only a one rule was hidden at a provided time, and this was treated as a disadvantage. Algorithm 1.b conceals the sensitive standards by diminishing their assist and sureness to small than minimum support limit or least certainty threshold. To make this, the exchanges that totally help the arrangement of parts in the right-hand side of the standard are picked and arranged in an increasing way subject to their length, and the right-hand side segment of the standard was removed from the exchange with sensitivity maximum. The extension in the count of sensitive rules results in a development in the count of lost rules in this algorithm [3].

Oliveira and Zaiane had an issue of hiding multiple sensitive association rules. The algorithms proposed consolidate IGA, Naïve, MaxFIA, and MinFIA that play out the hiding methodology by verifying double the database. Initially, this algorithm detects sensitive exchanges and noted them in order to extend the speed of sensitive exchange detections. Then, consequent to removing the chosen component, sanitization was executed with a less amount of sing components [4].

DSR and ISL algorithms were proposed by Wang et al. The two algorithms rely upon the records deforming strategy. ISL algorithm covers the sensitive rules through diminishing the sureness of sensitive standards to not exactly least certainty threshold, by extending their assist for the left-hand side component. DSR algorithm conceals the sensitive rules by diminishing their conviction to low than least certainty threshold, by reducing their assist for the right-hand side component. ISL algorithm was poor in the amount of hiding errors and DSR algorithm was feeble in the amount of lost rules [12].

Dehkordi, M. N., et al., Utilized a GA to give another technique to hide sensitive association standards. Notwithstanding hiding sensitive rules, the primary objective of algorithm has to decrease the modifications in the database. So as to accomplish this objective, this algorithm characterizes a pre-processing phase in that just delicate exchanges of the database are chosen and modifications are just done on delicate exchanges. Likewise, in the algorithm, 4 various procedures for fitness capacities are presented to hide sensitive standards and sensitive records with less drawbacks [6].

Khan et al. characterized a fitness function to enhance the methodology that was presented by Dehkordi [6]. In this strategy, notwithstanding endeavors to lessen the error in hiding, ghost rules and lost rules, a new measure known as the records loss, was additionally concerned [21].

Afshari et al. utilized a Cuckoo optimization for sensitive association rules hiding. In this technique, the hiding procedure was executed by the records distortion strategy. Likewise, in this strategy, three functions of fitness were utilized to accomplish an ideal technique with the fewer drawbacks. A pre-processing task was executed on the first database, so just exchanges with delicate records could be associated with the hiding procedure [8].

Le et al. proposed a heuristic algorithm dependent on the intersecting grid of successive record sets for sensitive rules hiding. The algorithm initially decides the victim records which changing these records created minimal effect on the set of regular recordsets. At that point, the minimum number of exchanges that should be altered was indicated. From that point onward, the victim records were expelled from the predetermined exchanges and the dataset was sanitized. Lin et al. have presented the two new algorithms, specifically, MSUMRU and MSU-MRU was independently wanted to confine the responses of the sanitization strategy for covering SHUIs [10].

Telikani et al. have explored 54 logical algorithms and reviewed them as far as 4 parameters comprising hiding technique, sanitization strategy, and determination technique. As far as results and discoveries, this review demonstrated a contrast with different parts of sanitization algorithms, the exchange and records determination strategies impact the optimal of hiding procedure and blocking method expands the exposure risk when distortion method was best in knowledge field of protection, exchange and insertion/deletion strategies [11].

III. STATEMENT OF PROBLEM

The issue of associated rules hiding could be characterized as the change of the real database into a sanitization database in order that the method of data mining were not fit for mining the database’s sensitive rules, though all non-sensitive tenets could be extricated. The common meaning of the issue is as per the following [17]: as for the exchanges of database D, slight change can be done on the minimum threshold of support, i.e. as opposed to giving regular threshold support, individual support is relegated for every records in the transactional database so as to detect the precise and progressively number of regular records which will produce the more number of sensitive rules Rs out of D, R subset is made as Rs sensitive rules, for hiding which is indicated by the proprietor of the database. The issue is which sanitization database D' must be framed such that every sensitive rule in Rs could not be extricated, though all non-sensitive standards in D could be extricated from D' [24]. The reason for hiding association rules is to address the accompanying necessities:

- The database of sanitization must not to permit any extrication of sensitive rules.
- The database of sanitization must permit the extrication of non-sensitive rules.
- A database of sanitization must not to create any new rule which does not present in D.

For hiding an association rule, that is sufficient just to have the help or certainty stage underneath the low threshold. Subsequently, so as to decrease the assist or certainty of the rules, the algorithms of association rules hiding search to deform the database and create modifications to it.

IV. EXISTING METHODOLOGY

4.1 Artificial Bee Colony Optimization

Generally, the algorithm of ABC comprises of 3 stages for total iteration of the search. The initial process is transferring the employed bees towards to their sources of food and assessing their levels of nectar.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Subsequent to sharing the food sources nectar records, the determination of food source zone through the spectators and assessing the nectar measure of the source of food is the second process. The last process is deciding the scout bees and afterward transferring them arbitrarily towards to conceivable new sources of food. In this research, the progression of the search is start the transaction, records that contain both non-sensitive and sensitive records and the count of changes needed to change over delicate records into non-sensitive records [27].

The second step comprises of computing the cost (total nectar), fitness function and likelihood to locate the better source of food zone for spectator and employed bees. The last process is deciding the relinquished source of food for scout bees and arbitrarily choosing the conceivable exchange based upon likelihood estimation and in sensitive records, one will be interchanged as zero. Regular records in the sensitive exchanges are adjusted as irregular. For each change, the count of change of sensitive records was decreased. The records has the most count of changes are chosen initially for change than various records. This procedure has proceeded unless the count of change becoming zero [27]. At last using the algorithm ECLAT in the changed database, no continuous records are recovered and furthermore, the sensitive standards have additionally hidden out of the database [26]. Concerning the real dataset needed just changes are made by the algorithm. No additional change was made and the records are not missed. It guarantees no fake rules are produced [25].

4.2 Grey Wolf Optimization Algorithm for Association Rule Hiding

4.2.1 Generating Initial Population

Grey Wolf optimization algorithm randomly produces an underlying population. Every individual from this population demonstrates records. Each one of the records in the underlying population shows a key for the database of sanitization which is a succession of zero and one. The existence and non-existence of records in the exchange are set apart by one and zero, separately. The initial key process in the underlying population is a collection of exchanges out of the real database which has been chosen in the pre-processing activity and completely helps at least 1 or many sensitive rules. To create randomly different solutions, just the delicate records that have been indicated in the pre-processing task modify with zero or one, and different ones stay unaltered and are sent to different solutions.

```
Pseudo Code for GWO
Input
Step 1: initialize the parameters P, S, Nt, Nm, Ne
P-Total no of transactions
S- Total no of records in the transaction
Nt –No of transactions with sensitive records
Nm –No of modifications
Ne –No of elimination
Output
Sanitized database
Step 2:  Association rule mining
i) From the given dataset find the frequent records by assigning individual threshold // IT is assigned to find the accurate and more number of frequent records.
ii) From the frequent records association rules are identified from minimum support and confidence.
iii) Rules are identified from this sensitive rules are identified //records which has more support and confidence value they are assumed as sensitive records.
Step 3: Association rule hiding
i) Association rules are taken as input in ARH.
ii) Sensitive records are identified.
Step: 4: Hunting prey
i) To identify the more number of sensitive records in transactions in this step a formula is used to find the more number of sensitive records
ii) P (i) =No of records present-No of non-sensitive records Total no of transactions.
iii) Apply this formula in all the transactions to find the highest number of sensitive records in the transactions.
iv) Arrange the transactions in the descending order
Step: 5 Modifications
i) In this step, by using the formula
Ns   = [No of occurrence (I1) – (IT -1)] // individual threshold value is set here to find accurate frequent records.
Identifies the number of modification to be done in each sensitive record.
Step 6: Elimination
i) Records are modified from the highest order transaction number
ii) Repeat this step until all the sensitive records are modified
iii) Modified records are stored in sanitized database.
```

4.2.2 Assess the Fitness Function- Hunting Prey

In this part, the estimation of the fitness function to every key process in the underlying population is determined. To make this, initially, every solution is converged with non-sensitive exchanges in the real database to know the effect of every key process on the whole real database. Consequently, the estimation of the received fitness function shows the general condition of the database of sanitization. It must be noticed which computing the fitness estimation to the primary solution in the underlying population was not important. As examined in the past stage, the primary solution comprises of the first database exchanges which have been displayed in the underlying population. The value of fitness for different solutions is determined to utilize fitness work which is clarified beneath. Where p represents the total number of transactions when the records are recognized all the records are organized in the maximum order then the transaction which has large number of sensitive records are taken first to do the alteration.

4.2.3 Generate Modifications

The technique for creating another solution in the algorithm proposed depends on the GWO algorithm and search technique.

That is subsequent stage Swamming is utilized to observe the no of alteration to be done in the particular records and adjust the sensitive records in the transaction. Swamming is utilized to detect the number of change. When the sensitive records are chosen for adjustment the event of the records is decreased with an individual threshold of the particular sensitive records – 1, which represents the number of change should be possible in the specific records.

4.2.4 Generating New Solutions- Elimination

The following step in the method is to change the sensitive records from the transaction. Weightage of every records and the quantity of sensitive records in a transaction are determined utilizing the past two steps. Here the transaction which has the more number of sensitive records will be given first chance to do the change. The sensitive records will be changed to lessen the number of events so that the record has hidden. These methods proceeded until all the sensitive records are changed and finished.

4.2.5 Updation of records

The last step is to make another sanitized database with the changed sensitive records. The Original database is approved with the changed database. It must fulfill the recently examined criteria of association rule hiding PPARM.

5. Description of Performance Evaluation and Dataset

5.1 Datasets

Table.1. Features of Dataset

Dataset	No of Transaction	No of Records	Avg. length of Records
Mushroom	8124	119	32
Chess	3196	75	23
Connect	15121	49	31
T100	100	37	20

So as to assess the abilities, qualities, and shortcomings of the proposed algorithm, different genuine databases have been utilized. Accordingly, to do the analysis, four datasets for example mushroom, connect, chess andT100 are taken from FIMI archive. The database features have appeared in Table.1.

5.2 Performance Measures

In terms for analyzing the hiding conditions, its reactions should be determined on the database. The procedure of hiding has many reactions. Accordingly, the assessment standards for computing these drawbacks were portrayed [25].

- HF(Hiding Failure): This model portrays the quantity of sensitive standards which the algorithm of sanitization neglected to hide, and they can, in any case, be extricated out of the database of sanitization D'. The estimation of HF is determined through the accompanying association: In this association, | Rs (D') | shows the quantity of sensitive standards extricated out of the database of sanitization D' and | Rs (D) | demonstrates the amount of delicate standards extricated out of the real database D [19].
- LR(Lost Rules): This paradigm demonstrates the amount of non-sensitive standards which are covered by the procedure of sanitization and could not be extricated from the database of sanitization D'. The estimation of LR was determined through the accompanying association: In this association, | ~ Rs (D) | demonstrates the quantity of non-sensitive standards extricated out of the real database D and | ~ Rs (D') | shows the quantity of non-sensitive standards extricated out of the database of sanitization D 20. [20].
- GR (Ghost Rules): This rule describes the count of rules which does not present on the real database D and were made as a result of the sterilization procedure and could be extricated out of database D'. The estimation of GR is determined. In this association, | R'| demonstrates this relation, the count of standards separated out of the database of sanitization D' and | R | portrays the count of standards extricated out the real database D [21].
- Runtime: The period of duration that algorithm takes to achieve the optimal solution.
- Memory: The total of storage space involved by the algorithm.

V. EXPERIMENTAL RESULTS

6.1 Comparing the efficiency

So as to analyze the proposed algorithm's efficiency with existing algorithms, sensitive records are chosen out of the transactions that have been extricated by the proposed algorithm with a slight change. Tables.2 and 3 demonstrates the comparative assessment on different dataset. Fig.1 and 2 demonstrate the Analysis of ghost rules, lost rules, hiding failure for the algorithm proposed and various algorithms, in chess, mushroom, T100, connect databases. The hiding error of BFO algorithm has small quantity of failures contrasting with various algorithms.

Table.2 Comparative Evaluation

Dataset	Algorithm	Efficiency Evaluation		
		Hiding Failure	Ghost Rules	Lost Rules
Mushroom	GWO	30	42	11
	ABC	40	52	20
Connect	GWO	47	21	17
	ABC	63	28	14
Chess	GWO	23	43	9
	ABC	34	51	13
TK100	GWO	31	21	12
	ABC	39	29	17

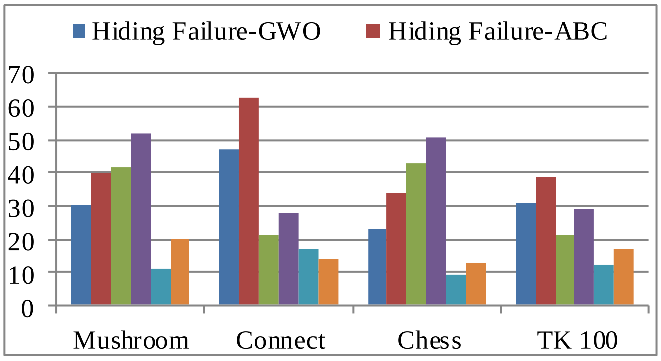

Figure.1. Graphical Representation of Efficiency Evaluation

6.2 Comparing the Runtime & memory space

The search technique in every algorithm is another compelling variable in the runtime. The GA utilizes two recombination and transformation activities in every redundancy. In this algorithm, in view of the algorithm parameters, various new solutions are made, which should be assessed. With respect to fitness capacity of this algorithm, assessing solutions may expand its runtime [28 – 32].

Table.3. Comparative Evaluation

Dataset	Algorithm	Performance Measures	
		Execution Time	Memory
Mushroom	GWO	11256	8386
	ABC	16090	11298
Connect	GWO	7321	5432
	ABC	8451	7345
Chess	GWO	10938	9028
	ABC	9394	9234
TK100	GWO	3920	1092
	ABC	4749	1239

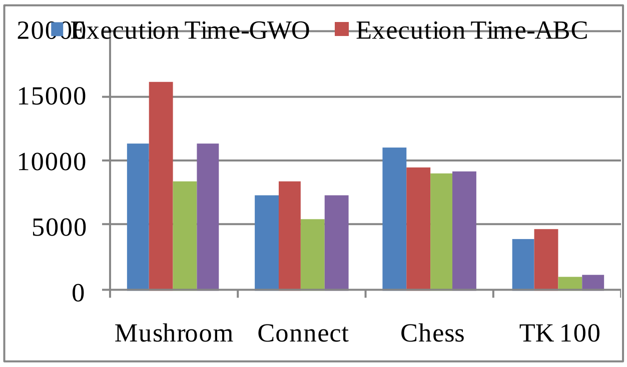

Figure.2. Graphical Representation of Performance Measures

VI. CONCLUSION

This research has presented a Metaheuristic strategy for sensitive association rules hiding utilizing an optimization algorithm. The algorithms presented were prepared to do hiding many sensitive records simultaneously. The most vital and compelling element of the current analysis is characterizing a preprocess activity which incorporates the value of Individual threshold to discover regular records accurately. In this examination, the proposed technique hides sensitive rules utilizing GWO. Many sensitive records are hidden at the same time in strategy. The proposed technique likewise has less lost rules over various algorithms. Fitness functions are implemented to discover the solution with few drawbacks. Fitness functions can decide the quantity of hiding errors and lost standards for every solution without data mining. Accordingly, in the algorithm GWO, data mining is executed just twice. Initially, the real database is inspected to decide sensitive and non-sensitive rules. Then next, the database of sanitization is analyzed. Hence computing the fitness to every solution, the fitness estimations of the solutions was correlated and total fitness estimations of different solutions so as to choose the better solution. The technique is assessed on both practical and synthetic datasets. The proposed methodology was correlated with ABC. From the analysis, the GWO is better when correlated with ABC.

REFERENCES

1. Berry, M. J., & Gordon S. Linoff. (2011). Data mining techniques for marketing, sales, and customer support. John Wiley & Sons, Inc.
2. Aggarwal, C. C., & Yu, P. S. (2004). A Condensation Approach to Privacy Preserving Data mining. In Adv In database Technology Edit 2004 Proc (Vol. 2992, pp. 183–199).
3. Verykios, V. S., Elmagarmid, A. K., Bertino, E., Saygin, Y., & Dasseni, E. (2004). Association rule hiding. IEEE Transactions on Knowledge and Records Engineering, 16(4), 434–447.
4. Oliveira, S. R. M., & Zaiane, O. R. (2002). Privacy-preserving frequent dataset mining. In Proceedings of the IEEE international conference on Privacy, security and data mining-Volume 14 (pp. 43–54).
5. Wang, L., Zheng, X., & Wang, S. (2013). A novel binary fruit fly optimization algorithm for solving the multidimensional knapsack problem. Knowledge-Based Systems, 48, 17–23.
6. Dehkordi, M. N., Badie, K., &Zadeh, A. K. (2009). A novel method for privacy preserving in association rule mining based on genetic algorithms. Journal of Software, 4(6).
7. Jia, D., Duan, X., & Khan, M. K. (2014). Binary Artificial Bee Colony optimization using bitwise operation. Computers & Industrial Engineering, 76, 360–365.
8. Afshari, M. H., Dehkordi, M. N., &Akbari, M. (2016). Association rule hiding using cuckoo optimization algorithm. Expert Systems with Applications, 64, 340–351.
9. Le, H. Q., Arch-Int, S., Nguyen, H. X., & Arch-Int, N. (2013). Association rule hiding in risk management for retail supply chain collaboration. Computers in Industry, 64(7), 776–784.
10. Lin, J. C.-W., Wu, T.-Y., Fournier-Viger, P., Lin, G., Zhan, J., & Voznak, M. (2016). Fast algorithms for hiding sensitive high utility recordsets in privacy-preserving utility mining. Engineering Applications of Artificial Intelligence, 55, 269–284.
11. Telikani, A & Shahbahrami, A. (2017). Records Sanitization in Association Rule Mining: An Analytical Review. Expert Systems.
12. Wang, S.-L., Parikh, B., &Jafari, A. (2007). Hiding informative association rule sets. Expert Systems with Applications, 33(2), 316–323.
13. Abedinpourshotorban, H., Shamsuddin, S. M., Beheshti, Z., &Jawawi, D. N. A. (2016). Electromagnetic field optimization: A Physics-inspired metaheuristic optimization algorithm. Swarm and Evolutionary Computation, 26, 8–22.
14. Atallah, M., Bertino, E., Elmagarmid, A., Ibrahim, M., &Verykios, V. (1999). Disclosure limitation of sensitive rules. In Proceedings - 1999 Workshop on Knowledge and Records Engineering Exchange, KDEX 1999 (pp. 45–52).
15. Awad, N. H., Ali, M. Z., Liang, J. J., Qu, B. Y., &Suganthan, P. N. (2016). Problem definitions and evaluation criteria for the CEC 2017 special session and competition on single objective bound constrained real-parameter numerical optimization. In Technical Report. NTU, Singapore.
16. Derrac, J., García, S., Molina, D., & Herrera, F. (2011). A practical tutorial on the use of nonparametric statistical tests as a methodology for comparing evolutionary and swarm intelligence algorithms. Swarm and Evolutionary Computation, 1(1), 3–18.
17. Gkoulalas-Divanis, A., &Verykios, V. S. (2010). Association rule hiding for data mining (Vol. 41). Springer Science & Business Media.
18. Holland, J. H. (1992). Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. MIT press.
19. Jain, D., Khatri, P., Soni, R., & Chaurasia, B. K. (2012). Hiding sensitive association rules without altering the support of sensitive record(s). In Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST (Vol. 84, pp. 500–509).
20. Kennedy, J., &Eberhart, R. C. (1997). A discrete binary version of the particle swarm algorithm. In Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation, 1997 IEEE International Conference on (Vol. 5, pp. 4104–4108).
21. Khan, A., Qureshi, M. S., &Hussain, A. (2014). Improved genetic algorithm approach for sensitive association rules hiding. World Applied Sciences Journal, 31(12), 2087–2092.
22. Mahmoudi, S., Rajabioun, R., &Lotfi, S. (2013). Binary cuckoo optimization algorithm. In 1 st National Conference on New Approaches in Computer Engineering and Information Retrieval Young Researchers And Elite Club of the Islamic Azad University, Roudsar-Amlash Branch.
23. Nouri, H., & Hong, T. S. (2012). A bacteria foraging algorithm based cell formation considering operation time. Journal of Manufacturing Systems, 31(3), 326–336.
24. Rashedi, E., Nezamabadi-Pour, H., &Saryazdi, S. (2010). BGSA: binary gravitational search algorithm. Natural Computing, 9(3), 727–745.
25. Verykios, V. S., & Gkoulalas-Divanis, A. (2008). A survey of association rule hiding methods for privacy. In Privacy-Preserving Data mining (pp. 267–289). Springer.
26. Yan, H., Yuan, X., Yan, S., & Yang, J. (2011). Correntropy based feature selection using binary projection. Pattern Recognition, 44(12), 2834–2842.

27.S.Vijayarani & M.Sathiya Prabha November 2011 Association Rule Hiding using Artificial Bee Colony Algorithm International Journal of Computer Applications (0975 – 8887) Volume 33– No.2.

28.Rajendran T and Sridhar K P. (2018). Epileptic seizure classification using feed forward neural network based on parametric features. International Journal of Pharmaceutical Research. 10(4): 189-196.

29.Hariraj V, et al. (2018). Fuzzy multi-layer SVM classification of breast cancer mammogram images. International Journal of Mechanical Engineering & Technology. 9(8): 1281-1299.

30.Rajendran T and Sridhar K P. (2019a). Epileptic Seizure-Classification using Probabilistic Neural Network based on Parametric Features. Journal of International Pharmaceutical Research. 46(1): 209-216.

31.Emayavaramban G, et al. (2019). Identifying User Suitability in sEMG Based Hand Prosthesis Using Neural Networks. Current Signal Transduction Therapy. DOI: 10.2174/1574362413666180604100542. (Article in Press).

32.Rajendran T and Sridhar K P. (2019b). An Overview of EEG Seizure Detection Units and Identifying their Complexity- A Review. Current Signal Transduction Therapy. DOI: 10.2174/1574362413666181030103616. (Article in Press).

AUTHORS PROFILE

Mrs.S.Sharmila, is pursuing her Ph.D in Department of Computer Science, Bharathiar University, Coimbatore, and Tamilnadu, India. She has completed M.C.A in Bharathiar University, Tamilnadu, India. Her research area includes Association Rule Mining, Association Rule Hiding, Privacy Preserving and Optimization techniques. She has published papers in International Journals and Conferences.

Dr. S.Vijayarani Mohan is an Assistant Professor of Department of Computer Science at Bharathiar University, Coimbatore, India. She has obtained M.C.A., M.Phil., and Ph.D., in Computer Science. She has 10 years of teaching/research and 10 years of technical experience. Her research interests include data mining, privacy issues in data mining, text mining, web mining, data streams and information retrieval. She has published more than 95 research articles in national/international journals. She also presented research papers in international/national conferences. She has authored a book and guided more than 25 research scholars. She is a life member in professional bodies like CSI, ISCA, IAENG, IRED and UACEE.