DOI: https://doi.org/10.46632/jemm/8/1/4

REST Journal on Emerging Trends in Modelling and Manufacturing
Vol: 8(1), 2022
REST Publisher; ISSN: 2455-4537
Website: www.restpublisher.com/journals/jemm

"CREDIT CARD FRAUD" DETECTION USING DATA ANALYTICS A COMPARATIVE ANALYSIS

***M. Ramkumar, R. Supriya, K. Chaithanya, J. Veena, A. SnehaLatha**
Department of Computer Science Engineering HKBK College of Engineering Bangalore, India.
*Corresponding author Email: ramkumar.cs@hkbk.edu.in.

Abstract. Fraud events take place frequently which results in a huge financial loss. Fraud detections are dynamic and are not easy to identity. Data mining plays a vital role in detection of "Credit card fraud" done in fraudulent online transactions. Fraudsters use latest advanced methods which is an advantage. This process becomes challenging based on two major reasons -firstly, the profiles of users keep changing constantly and secondly, the datasets required for this are highly confusing. The overall performance of "Credit card fraud" detections is improved by sampling approach on the dataset. This research looks at fraud incidents in the context of real-life fraud transactions. A variety of machine learning methods and modelling approaches are used to combat each fraud. The goal of this study is to see how well logistic regression and K-nearest neighbour (KNN) perform on highly skewed "Credit card fraud" data. In order to assess the algorithm's robustness even further, noise is injected into the data sets. The major purpose of this study is to compare and contrast numerous methods for identifying fraud.
Keywords: "Credit card fraud"; Fraud Detection; Data mining; real-time fraud transactions; Logistic Regression; K-nearest neighbor (KNN); comparative analysis

1. Introduction

It's a little, handy plastic card that contains personal information like a signature or a picture, and it allows the person whose name appears on it to charge products or services to his account, for which he will be charged on a regular basis. In order to deliver services, automated teller machines (ATMs), retail readers, banks, and online internet banking systems all read the information held on a credit or debit card. They have a unique card number that is very valuable to them. It relies on the physical security of the plastic card as well as the confidentiality of the credit card number to work effectively [1]-[12]. Credit card transactions are rapidly expanding, resulting in a huge rise in the number of persons participating in fraudulent activities. According to the Federal Trade Commission, "Credit card fraud" is a wide term that refers to theft and fraud involving the use of a credit card as a false source of money in a specific transaction [13]-[25]. In order to tackle the fraud detection problem, most statistical approaches and a range of data mining algorithms are applied. In "Credit card fraud" detection systems, artificial intelligence methods such as machine learning, meta learning, and pattern matching are employed. Genetic algorithms are a kind of evolutionary algorithm that is used to solve issues like fraud detection and prevention. The creation of an efficient and secure electronic payment system, which can be utilized to assess whether a transaction is fraudulent or not, is prioritized. In this post, we'll look at "Credit card fraud" and the steps you may take to avoid it. When someone uses another person's credit card for their own personal purpose without the owner's knowledge, this is referred to as "Credit card fraud". When fraudsters participate in this kind of behavior, the system is abused to the point that the whole allowable limit is depleted. As a consequence, we'd want a solution that lowers the credit card's overall credit limit, which is more open to fraud than the other possibilities. Furthermore, as time passes, a Genetic algorithm improves the problem's answers. The main aim is to create an efficient and secure electronic payment system, with the purpose of detecting fraudulent transactions as a secondary goal.

2. Related Works

As previously mentioned, the study's main focus is on assessing whether or not a transaction is fraudulent, implying that the problem is one of classification, which can be solved utilizing classification techniques.

"Credit card fraud"

"Credit card fraud" is a kind of identity theft in which someone falsely charges products to someone else's credit card account or withdraws money from that account using that person's credit card information. When it comes to "Credit card fraud", the fraudulent use of a debit card is also included. Theft of a credit card or unlawfully accessing the cardholder's account and personal information, such as the cardholder's name and address, and then using that information to make fraudulent transactions are two ways "Credit card fraud" may be committed. Various law enforcement agencies, ranging from local police departments to the US Secret Service, are vigorously enforcing fraud laws, notably those relating to "Credit card fraud". Consider the "Credit card fraud" definition below as an example of how to better comprehend this concept. Credit card theft happens when someone steals a credit or debit card or gets the card number and other account information required to use the card unlawfully. While physical "Credit card fraud" is possible, the regularity with which account

information is stolen electronically has increased dramatically thanks to modern technologies. Until the card information is used to make transactions, the account holder, the merchant from whom the card information was stolen or intercepted, and even the card issuer may be fully unaware of the breach [26]-[34]. Because of the growing popularity of online shopping and bill payment, having a physical credit card or debit card is no longer required to make transactions or pay bills. It's even possible to open a bank account just for the purpose of taking credit cards online. If thieves are successful in collecting enough personal information about other people, they may use it to conduct credit card fraud by opening new accounts or obtaining new cards to use on existing accounts.

Features and elements

Its elements may include: When someone acquires a credit card or credit card number from another person without their consent with the intent of using or selling the information, this is known as credit card theft. A credit card forgery is defined as the purchase of anything of value using a credit card by someone other than the cardholder or an authorized user with the intent of defrauding the credit card issuer: Credit card fraud is described as the use of a credit card or a credit card number with the goal of using, selling, or transferring the number to another person. "Credit card fraud" is described as using a credit card or card number to buy anything of value with the goal of misleading another person.

"Credit card fraud" detection

Some of the currently used approaches to detection of such fraud are:

- Artificial neural Network
- Fuzzy Logic
- Genetic Algorithm
- Logistic regression
- Decision Tree
- Support vector machines
- Bayesian Networks
- Hidden Markov Model
- K-Nearest Neighbor

Detection Process

Step 1: Separate each individual client's transactions from the aggregate transaction database's transactions.

Step 2: Separate the authorized and fraudulent transactions of a customer's databases from the transactions of all of his or her customers' databases.

Step 3: Applying a specified standard algorithm to a collection of legal transactions involving distinct consumers and determining the difference between the two transactions is the goal. The following diagram depicts the overall architecture of a "Credit card fraud" detection system, as well as the flow of a fraud detection process.

3. Experimental Setup and Methods

The data sets and classifications used in our research will be categorized using Logistic Regression techniques. Every stage of the implementation was done in Python, including libraries like NumPy, Pandas, Keras, Scikit-Learn, and Tensor flow. With the aid of Rstudio, data purification was done on occasion. PowerBI is also available for visualising the whole transactional process. The many stages of the transactions, which include data collection, data preparation, data analysis, classifier algorithm training, and classifier algorithm testing. The data is translated into a readable format and fit and sampled during the preparation stage. The dataset is subjected to feature selection and reduction throughout the analysis stage, which is achieved using PCA (Principal Component Analysis). During the training phase, classifier algorithms are built and fed with the processed data that will be used to classify the data. The effectiveness of the transactions is examined using True Positive, False Positive, True Negative, and False Negative replies to the questions in our research. The findings are compared, and the accuracy, sensitivity, specificity, and precision of these classifiers are evaluated [36]-[58].

Dataset

There are two days in September 2013 in which the dataset comprises transactions of European credit card users. Because of confidentiality concerns, the dataset contains the v1-v28 PCA feature as well as Time and Amount, which are well-known features and are classified as 0 and 1. The positive class accounts for 0.172 percent of the total transaction volume. An amalgamation of two data sources, the fraud transactions log file and the all transactions log file, was used to construct the dataset. A significant portion of the dataset is uneven and biased in favour of the positive class. There are 28 primary components as a consequence of the PCA feature selection procedures that were carried out. As a result, a total of 30 input characteristics are used in this investigation. When a transaction occurs, the time feature records the second that has passed between it and the very first transaction in the dataset. The 'amount' feature indicates the amount of the transaction. It is the target class for the binary classification that is represented by the 'class' feature, which takes the value 1 (positive case) to indicate fraud and the value 0 (negative case) to indicate non fraud.

Data Cleaning

The process of filling in missing data is an important part of the data cleaning method. There are a number of ways to solve this issue, including ignoring the whole tulle, but the bulk of them are likely to add bias into the findings. Furthermore, with changes such as the elimination of unnecessary columns and the separation of the date time column into two columns.

Data Integration

Because the fraudulent and real record files were originally housed in two separate files, the two data sources were integrated to preclude future data tampering.

Data Transformation

All of the information from the various categories was compiled into a numerical format that was simple to understand. The transactional dataset contains a variety of data types with a variety of ranges. As a consequence, data transformation entails data cleaning and normalization.

Data Reduction

In this example, the approach that was applied was dimension reduction. Principal component analysis, or PCA, is a well-known transform method that is frequently utilized in a variety of sectors. The application of this method handles the feature selection issue in question from the perspective of numerical analysis. Because PCA was able to find the ideal number of major components, it was helpful in feature selection.

Logistic Regression

An method that may be used for both regression and classification problems, however it is more often employed for classification jobs due to its simplicity. In Logistic Regression, the result is a binary that belongs to one of the classes that were defined. With the help of dependent variables, it is possible to predict categorical variables. This method is simple binary classification to two values, where it computes probability values ranging between (0) and (1) for each value (1). It determines the parameters that provide the greatest fit to a nonlinear function known as the sigmoid. Sigmoid Function (**σ**) or Logistic Function (L) are two terms used to describe a more complicated cost function used by this algorithm. An method that may be used for both regression and classification problems, however it is more often employed for classification jobs due to its simplicity. In Logistic Regression, the result is a binary that belongs to one of the classes that were defined. With the help of dependent variables, it is possible to predict categorical variables. This method is simple binary classification to two values, where it computes probability values ranging between (0) and (1) for each value (1). It determines the parameters that provide the greatest fit to a nonlinear function known as the sigmoid. Sigmoid Function (**σ**) or Logistic Function (L) are two terms used to describe a more complicated cost function used by this algorithm.

$$\sigma(x) = \frac{1}{(1+l\text{^}-1)}$$

$$X = WoZo + W1Z1 + \ldots\ldots + WnZn$$

The sigmoid function's input(x) is multiplied by the vector z, which represents the input data, and the best coefficients W. Each element is multiplied and combined together to generate a single value, which is used to determine the classifier's categorisation of the target class. It uses the logistic function to convert the x-values of the dataset's multiple occurrences into a range of 0 to 1. If the sigmoid's value is greater than 0.5, it becomes 1; otherwise, it remains 0. The gradient ascent is then calculated one by one for each feature value in the dataset. Given the large quantity of data in this study, gradient ascent is often used since it updates the weights using just one instance at a time, reducing the study's total computing complexity.

4. Conclusion

Because of the variation in fraud patterns that has happened over time, “Credit card fraud” detection has been an interesting area of research for many years. This research analyses and categorises whether a transaction is fraudulent or lawful using a classification system. It compares the performance of the algorithms and finds that the logistic regression model is much more effective and performs better than the others. On real-world credit card transaction data, a variety of machine learning algorithms, including k-nearest neighbour (KNN) and logistic regression, have been tried and taught. The findings of the experiment reveal that logistic regression performed substantially well in all of the experiments that were analysed. If these algorithms are trained with some reaso-nable information, this aspect of our system may enable us to make a judgement and go on to the next phase as soon as a fraudulent transaction is discovered. As a result, we can reach near-perfect accuracy using logistic regression; nevertheless, we are striving to obtain more accuracy with respect to data when we combine various methods that give us with greater accuracy. As a result, we'd achieve better accuracy, and by lowering the number of fraudulent transactions, we'd still be able to get the results using logistic regression, which we'll try in the future.

Acknowledgment (HEADING 5)

We wish to acknowledge Dr. M. RamKumar for his effort in the experimentation carried out and the team for the source and description of the "Credit card fraud" data.

References

[1]. Abhinav Srivastava, Amal Kundu, Shamik sural, Arun Majumdar - "Credit card fraud" Detection Using Hidden Markov Model IEEE 2008

[2]. Abrar Nadim , Ibrahim Mohammad Sayem , Aapan Mutsuddy ,Mohammad Sanaullah Chowdhury -Analysis of Machine Learning Techniques for "Credit card fraud" Detection IEEE 2019

[3]. CLIFTON PHUA1, VINCENT LEE1, KATE SMITH1 & ROSS GAYLER2 A Comprehensive Survey of Data Mining-based Fraud Detection Research published by School of Business Systems, Faculty of Information Technology, Monash University, Wellington Road,Clayton, Victoria 3800, Australia

[4]. John Richard D. Kho, Larry A. Vea -"Credit card fraud" Detection Based on Transaction Behaviour - published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017

[5]. Nikita Shirodkar , Pratiksha mandrekar,Rohit Shet Mandrekar , Rahul Sakhalkar, K.M. Chaman Kumar , Shailendra Aswale - "Credit card fraud" Detection Techniques IEEE 2020

[6]. Suman-Survey Paper on "Credit card fraud" Detection , Research Scholar, GJUS&T Hisar HCE, Sonepat published by International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014

[7]. S. H. Projects and W. Lovo, ―JMU Scholarly Commons Detecting "Credit card fraud" : An analysis of fraud detection techniques,‖ 2020.

[8]. N. R. Deepak and S. Balaji, "Performance analysis of MIMO-based transmission techniques for image quality in 4G wireless network," 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2015, pp. 1-5, doi: 10.1109/ICCIC.2015.7435774.

[9]. Loganathan, R., & Kumaraswamy, Y. S. (2013). Active contour based medical image segmentation and compression using biorthogonal wavelet and embedded zerotree. Indian Journal of Science and Technology, 6(4), 4390-4395.

[10]. Jotheeswaran, J., Loganathan, R., & Madhu Sudhanan, B. (2012). Feature reduction using principal component analysis for opinion mining. International Journal of Computer Science and Telecommunications, 3(5), 118-121.

[11]. Loganathan, R., & Kumaraswamy, Y. S. (2011, December). An improved active contour medical image compression technique with lossless region of interest. In 3rd International conference on trendz in information sciences & computing (TISC2011) (pp. 128-132). IEEE.

[12]. Loganathan, R., & Kumaraswamy, Y. S. (2010). Medical image compression using biorthogonal spline wavelet with different decomposition. IJCSE International Journal on Computer Science and Engineering, 2(9), 3003-3006.

[13]. Loganathan, R., & Kumaraswamy, D. Y. (2012). Medical Image Compression with Lossless Region of Interest Using Fuzzy Adaptive Active Contour. In International Conference on Computational Techniques and Mobile Computing (ICCTMC'2012) December (pp. 14-15).

[14]. Loganathan, R., & Kumaraswamy, Y. S. (2002). Performance Evaluation of Image Compression for Medical Image. International Journal of Advanced Research in Computer Science and Software Engineering [2013] Vol, 4.

[15]. Kurian, S., & Ramasamy, L. (2021). Securing Service Discovery from Denial of Service Attack in Mobile Ad Hoc Network (MANET). International Journal of Computer Networks and Applications, 8(5), 619-633.

[16]. Khan, Z., & Loganathan, R. (2020, October). AutoLiv: Automated Liver Tumor Segmentation in CT Images. In 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE) (pp. 151-156). IEEE.

[17]. Loganathan, R., Khan, F. A., Gulzar, I., Parray, I. N., & Bhat, F. A. (2020). A Survey on Prober: An automated network vulnerability scanner. International Scientific Journal of Contemporary Research in Engineering Science and Management, 5(2), 85-88.

[18]. Loganathan, R., Aliya, B. B., Rehman, S. S. U., & Pasha, A. (2020). A Survey on Paperless Examination. International Scientific Journal of Contemporary Research in Engineering Science and Management, 5(2), 80-84.

[19]. Khan, Z. (2020). Radiomics in Prostate MRI: A Review on Opportunities & Challenges. International Scientific Journal of Contemporary Research in Engineering Science and Management, 5(1), 7-10.

[20]. Kurian, S., & Ramasamy, L. (2021). Novel AODV based service discovery protocol for MANETS. Wireless Networks, 27(4), 2497-2508.

[21]. Patan, R., & Gandomi, A. H. (2021). Improved salient object detection using hybrid Convolution Recurrent Neural Network. Expert Systems with Applications, 166, 114064.

[22]. Yuvaraj, N., Srihari, K., Dhiman, G., Somasundaram, K., Sharma, A., Rajeskannan, S., ... & Masud, M. (2021). Nature-InspiredBased Approach for Automated Cyberbullying Classification on Multimedia Social Networking. Mathematical Problems in Engineering, 2021.

[23]. Natarajan, Y., Kannan, S., & Mohanty, S. N. (2021). Survey of Various Statistical Numerical and Machine Learning Ontological Models on Infectious Disease Ontology. Data Analytics in Bioinformatics: A Machine Learning Perspective, 431-442.

[24]. Raja, R. A., Yuvaraj, N., & Kousik, N. V. (2021). Analyses on Artificial Intelligence Framework to Detect Crime Pattern. Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 119-132.

[25]. Kannan, S., Dhiman, G., Natarajan, Y., Sharma, A., Mohanty, S. N., Soni, M., ... & Gheisari, M. (2021). Ubiquitous Vehicular AdHoc Network Computing Using Deep Neural Network with IoT-Based Bat Agents for Traffic Management. Electronics, 10(7), 785.

[26]. Yuvaraj, N., Raja, R. A., Karthikeyan, T., & Kousik, N. V. (2020). 11 Improved Privacy Preservation Framework for Cloud-Based Internet of Things. Internet of Things: Integration and Security Challenges, 165.

[27]. Yuvaraj, N., Karthikeyan, T., & Praghash, K. (2021). An improved task allocation scheme in serverless computing using gray wolf Optimization (GWO) based reinforcement learning (RIL) approach. Wireless Personal Communications, 117(3), 2403-2421.

[28]. Mariappan, L. T., & Yuvaraj, N. (2020). Analysis On Cardiovascular Disease Classification Using Machine Learning Framework. Solid State Technology, 63(6), 10374-10383.

[29]. Karthick, S., Yuvaraj, N., Rajakumari, P. A., & Raja, R. A. (2021). Ensemble Similarity Clustering Frame work for Categorical Dataset Clustering Using Swarm Intelligence. In Intelligent Computing and Applications (pp. 549-557). Springer, Singapore.

[30]. Yuvaraj, N., Raja, R. A., & Kousik, N. V. (2021). Privacy Preservation Between Privacy and Utility Using ECC-based PSO Algorithm. In Intelligent Computing and Applications (pp. 567-573). Springer, Singapore.

[31]. Yuvaraj, N., Raja, R. A., Palanivel, P., & Kousik, N. V. (2020, April). EDM Process by Using Copper Electrode with INCONEL 625 Material. In IOP Conference Series: Materials Science and Engineering (Vol. 811, No. 1, p. 012011). IOP Publishing.

[32]. Veerappan Kousik, N. G., Natarajan, Y., Suresh, K., Patan, R., & Gandomi, A. H. (2020). Improving Power and Resource Management in Heterogeneous Downlink OFDMA Networks. Information, 11(4), 203.

[33]. Natarajan, Y., Raja, R. A., Kousik, D. N., & Johri, P. (2020). Improved Energy Efficient Wireless Sensor Networks Using Multicast Particle Swarm Optimization. Available at SSRN 3555764.

[34]. Khadidos, A., Khadidos, A. O., Kannan, S., Natarajan, Y., Mohanty, S. N., & Tsaramirsis, G. (2020). Analysis of COVID-19 Infections on a CT Image Using DeepSense Model. Frontiers in Public Health, 8. 20.

[35]. Yuvaraj, N., Srihari, K., Chandragandhi, S., Raja, R. A., Dhiman, G., & Kaur, A. (2021). Analysis of protein-ligand interactions of SARS-Cov-2 against selective drug using deep neural networks. Big Data Mining and Analytics, 4(2), 76-83.

[36]. Yuvaraj, N., Karthikeyan, T., Praghash, K., & Reddy, K. H. (2021). Binary flower pollination (BFP) approach to handle the dynamic networking conditions to deliver uninterrupted connectivity. Wireless Personal Communications, 121(4), 3383-3402.

[37]. Maheshwari, V., Mahmood, M. R., Sravanthi, S., Arivazhagan, N., ParimalaGandhi, A., Srihari, K., ... & Sundramurthy, V. P. (2021). Nanotechnology-Based Sensitive Biosensors for COVID-19 Prediction Using Fuzzy Logic Control. Journal of Nanomaterials, 2021.

[38]. Natarajan, Y., Kannan, S., Selvaraj, C., & Mohanty, S. N. (2021). FORECASTING ENERGY GENERATION IN LARGE PHOTOVOLTAIC PLANTS USING RADIAL BELIEF NEURAL NETWORK. Sustainable Computing: Informatics and Systems, 100578.

[39]. Natarajan, Y., Raja, R. A., Kousik, N. V., & Saravanan, M. (2021). A review of various reversible embedding mechanisms. International Journal of Intelligence and Sustainable Computing, 1(3), 233-266.

[40]. Kousik, N. V., Sivaram, M., Yuvaraj, N., & Mahaveerakannan, R. (2021). Improved Density-Based Learning to Cluster for User Web Log in Data Mining. In Inventive Computation and Information Technologies (pp. 813-830). Springer, Singapore.

[41]. Yuvaraj, N., Praghash, K., & Karthikeyan, T. (2021). Data Privacy Preservation and Trade-off Balance Between Privacy and Utility Using Deep Adaptive Clustering and Elliptic Curve Digital Signature Algorithm. Wireless Personal Communications, 1-16.

[42]. Arivazhagan, N., Somasundaram, K., Vijendra Babu, D., Gomathy Nayagam, M., Bommi, R. M., Mohammad, G. B., ... & Prabhu Sundramurthy, V. (2022). Cloud-Internet of Health Things (IOHT) Task Scheduling Using Hybrid Moth Flame Optimization with Deep Neural Network Algorithm for E Healthcare Systems. Scientific Programming, 2022.

[43]. Gobinathan, B., Mukunthan, M. A., Surendran, S., Somasundaram, K., Moeed, S. A., Niranjan, P., ... & Sundramurthy, V. P. (2021). A Novel Method to Solve Real Time Security Issues in Software Industry Using Advanced Cryptographic Techniques. Scientific Programming, 2021.

[44]. Yuvaraj, N., Raja, R. A., Karthikeyan, T., & Praghash, K. (2021). Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) Using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack. Wireless Personal Communications, 1-17.

[45]. Yuvaraj, N., Praghash, K., Raja, R. A., & Karthikeyan, T. (2021). An Investigation of Garbage Disposal Electric Vehicles (GDEVs) Integrated with Deep Neural Networking (DNN) and Intelligent Transportation System (ITS) in Smart City Management System (SCMS). Wireless Personal Communications, 1-20.

[46]. Kumar, A. S., Jule, L. T., Ramaswamy, K., Sountharrajan, S., Yuuvaraj, N., & Gandomi, A. H. (2021). Analysis of false data detection rate in generative adversarial networks using recurrent neural network. In Generative Adversarial Networks for Image-to-Image Translation (pp. 289-312). Academic Press.

[47]. Pradeep, P., J. Edwin Raja Dhas, M. Ramachandran, and B. Stanly Jones Retnam. "Mechanical Characterization of jute fiber over glass and carbon fiber reinforced polymer composites." International Journal of Applied Engineering Research 10, no. 11 (2015): 10392-10396.

[48]. Sangeetha, S. B., Sabitha, R., Dhiyanesh, B., Kiruthiga, G., Yuvaraj, N., & Raja, R. A. (2022). Resource Management Framework Using Deep Neural Networks in Multi-Cloud Environment. In Operationalizing Multi-Cloud Environments (pp. 89-104). Springer, Cham.

[49]. Gowrishankar, J., Kumar, P. S., Narmadha, T., & Yuvaraj, N. (2020). A Trust Based Protocol For Manets In Iot Environment., International Journal of Advanced Science and Technology 29 (7), 2770-2775.

[50]. Karthick, S., Yuvaraj, N., Rajakumari, P. A., & Raja, R. A. (2021). Ensemble Similarity Clustering Frame work for Categorical Dataset Clustering Using Swarm Intelligence. In Intelligent Computing and Applications (pp. 549-557). Springer, Singapore.

[51]. Yuvaraj, N., Raja, R. A., & Kousik, N. V. (2021). Privacy Preservation Between Privacy and Utility Using ECC-based PSO Algorithm. In Intelligent Computing and Applications (pp. 567-573). Springer, Singapore.

[52]. Daniel, A., Kannan, B. B., Yuvaraj, N., & Kousik, N. V. (2021). Predicting Energy Demands Constructed on Ensemble of Classifiers. In Intelligent Computing and Applications (pp. 575-583). Springer, Singapore.

[53]. Yuvaraj, N., Raja, R. A., Kousik, N. V., Johri, P., & Diván, M. J. (2020). Analysis on the prediction of central line-associated bloodstream infections (CLABSI) using deep neural network classification. In Computational Intelligence and Its Applications in Healthcare (pp. 229-244). Academic Press.

[54]. Sangeetha, S. B., Blessing, N. W., Yuvaraj, N., & Sneha, J. A. (2020). Improving the training pattern in back-propagation neural networks using holt-winters' seasonal method and gradient boosting model. In Applications of Machine Learning (pp. 189-198). Springer, Singapore.

[55]. Natarajan, Y., Raja, R. A., Kousik, D. N., & Johri, P. (2020). Improved Energy Efficient Wireless Sensor Networks Using Multicast Particle Swarm Optimization. Available at SSRN 3555764.

[56]. Yuvaraj, N., Kousik, N. V., Jayasri, S., Daniel, A., & Rajakumar, P. (2019). A survey on various load balancing algorithm to improve the task scheduling in cloud computing environment. J Adv Res Dyn Control Syst, 11(08), 2397-2406.

[57]. Yuvaraj, N., Chang, V., Gobinathan, B., Pinagapani, A., Kannan, S., Dhiman, G., & Rajan, A. R. (2021). Automatic detection of cyberbullying using multi-feature based artificial intelligence with deep decision tree classification. Computers & Electrical Engineering, 92, 107186.

[58]. Natarajan, Y., Kannan, S., & Dhiman, G. (2021). Task scheduling in cloud using aco. Recent Advances in Computer Science and Communications, 13, 1-6.

