PROCEEDINGS OF

INTERNATIONAL CONFERENCE ON ADVANCED TECHNOLOGIES

https://proceedings.icatsconf.org/

11th International Conference on Advanced Technologies (ICAT'23), Istanbul-Turkiye, August 17-19, 2023.

Detection of Credit Card Fraud with Artificial Neural Networks

Ferhat YEŞİLYURT[1], Hasan TEMURTAŞ[2], Çiğdem BAKIR[3]

[1]Graduate School of Education, Com. Department, Kutahya Dumlupinar University , Kutahya, TURKEY
ferhat.yesilyurt@ogr.dpu.edu.tr, ORCID: 0000-0002-4119-3318

[2]Computer Engineering Department, Kutahya Dumlupinar University , Kutahya, TURKEY
hasan.temurtas @dpu.edu.tr, ORCID: 0000-0001-6738-3024

[3]Software Engineering Department, Kutahya Dumlupinar University , Kutahya, TURKEY
cigdem.bakir@dpu.edu.tr, ORCID: 0000-0001-8482-2412

Abstract— **Along with the Internet, digital technologies are frequently used in every moment of our lives. Many transactions that we carry out in monetary terms such as shopping in our daily life are now done digitally. With the developing digitalization in the world, people's lives become easier and people can access different products in a short time. In particular, people can spend and shop quickly and easily without carrying cash in their pockets with a credit card. However, with the increase in the use of credit cards, there are also some security vulnerabilities. Fraudsters can gain unfair advantage by obtaining certain credit card information such as passwords. They can shop with someone else's credit card without permission. These transactions cause substantial financial damage to individuals and institutions. With the increase in the use of credit cards with the developing technology, such credit card fraud is also increasing rapidly. Taking precautions against credit card fraud is a very important issue in order to ensure the safety of people. For this reason, in order to ensure the security of both banks and financial institutions that provide credit card services, it is necessary to prevent credit card fraud and to detect fraud that may occur in credit cards within the scope of combating fraud. In our study, Artificial Neural Networks were used to detect credit card fraud transactions. A prediction model has been developed to detect fraud in credit card transactions with ANN. Using the Credit Card data set obtained from the Kaggle database, modeling was done with the Feed Forward Artificial Neural Network method. The aim of this study is to automatically detect abnormal behaviors made with credit cards. 98.44% success was achieved with feedforward artificial neural network.**

Keywords— **ANN, credit card, fraud, feed forward, confusion matrix**

I. INTRODUCTION

Today, with the rapid increase in the widespread use of the internet, many companies, institutions and organizations have started to carry out their activities online. Especially, financial companies have started to conduct most of their transactions online in order to save time and make fast transactions[1]. Especially in recent years, many institutions and individuals have been doing their online shopping (market, white goods, television purchase, fuel, etc.) and all other transactions with debit and credit cards in order to provide cash transfer. Generally, large hotels and various car rental companies may require the buyer to make transactions with a credit card. People even pay their bills via bank or credit card. However, there are some disadvantages as well as these advantages of online transactions. Especially in many institutions such as banking and finance companies, fraud and illegal activities are increasing rapidly due to online transactions[2].

Fraud detection related to the use of bank and credit cards can be handled in many ways[3]: The most common and common ones are ATM fraud and the operation of card information, account redirection, online shopping and copying of card information. It is very important for the security of individuals and institutions to detect different transactions and movements on these accounts. Because, in terms of data security and privacy, the transfer of bank and credit card information to other people and their misuse is becoming a very serious problem today. Fraudsters can capture people's information from e-commerce sites and copy this information for different purposes. Credit card fraud causes financial losses all over the world and researchers are trying to prevent credit card fraud with various data analyzes.

Credit card fraud is a growing problem in many areas such as banking and online shopping. Especially credit card fraudsters develop new strategies and engage in illegal transactions. These illegal transactions cause consumers and financial institutions to lose money every day. In our study, we proposed a model that detects attacks on credit card transactions in order to prevent these illegal transactions and to transfer data securely with credit cards. The scientific contribution of our study is to detect credit card fraud and prevent the elements that will threaten data security. In our study, the dataset used for the detection of abnormal behavior in credit card transactions or fraud detection was trained with artificial neural networks, and the success and performance results were discussed in detail, and what kind of work to be included in the future was determined by evaluating the results.

II. Related Works

Recent developments in online payment technologies are increasing, especially with COVID-19. With this global epidemic, people generally started to shop for products online and with credit cards. This naturally led to a significant increase in credit card fraud. In particular, the banking, finance and industrial sectors were adversely affected. Various studies have been carried out for online product exchange, data integrity of individuals and institutions, and accurate and reliable transactions. These studies are given below:

Belle et al. proposed the CATCHM method for fraud detection, which is based on RL (Representation Learning) network-based credit card fraud detection[4]. The RL technique tries to determine the relationships between innovative network design and credit card transactions against the situations that may occur in the network. In this study, a more efficient and effective detection model is presented based on relationships. In addition, they evaluated the results temporally in order to realize the negative situations in the network. They found future activities using digital traces of data for fraud detection. In this study, data analytics was prioritized. In addition, CATCH, a network-based fraud detection method, has been proposed. This method is based on the relationships between transactions performed in the database and adopts the representative learning method in credit card data. In the study, firstly, the network design was carried out for the dataset. An optimization approach is proposed for the inductive pooling extension.

Jovanovic et al. used hybrid machine learning methods to prevent the increase in credit card fraud due to the impact of COVID-19 and to detect fraud[5]. They also compared the success of the methods by applying the developed metaheuristic and herd intelligence methods on the real data set. Firefly algorithm was applied on synthetic and real credit dataset and classification success was evaluated. However, more parameters need to be determined in order to evaluate the study with more datasets and to evaluate the methods used.

In order to detect credit card fraud, Xie et al. tried to detect possible fraudulent behavior by looking at the activities based on the past transactions of the users[6]. In this study, they tried to determine the behavioral changes caused by the sequential transactions of the users with the time sensitive LSTM (Long short term memory) method. The time differences between the two transactions die the behavioral response of the users in the use of the credit card, and the reactions determine the future behavior of the users.

Roseline et al., on the other hand, developed an iterative neural network that determines long and short-term behaviors in order to prevent financial losses caused by credit card fraud that has increased in recent years[7]. This neural network and Support Vector Machines used in the literature were compared with various machine learning algorithms such as Naive Bayes and artificial neural networks, and the success of the proposed model was presented comparatively. They also tried to automatically identify processes and events that may arise in case of fraud. The performance of the proposed model was calculated by considering criteria such as precision, accuracy, precision and error rate. However, in this study, the detection of long-term fraud is not discussed and the detection of long-term fraud has not been fully realized.

Alfaiz et al. tried to detect credit card fraud in two stages in order to prevent fraud with the increasing dependency on credit cards, which are carried out online[8]. Many methods such as decision trees, CatBoost, XGBoost, Random Forest, using different combinations of up and down sampling have been applied to the credit card dataset. Each model's success was measured by k-fold crossover validation. In the first stage, 9 machine learning methods were used, and in the second stage, 19 resampling techniques were used. However, they need to test the success of their proposed model on more datasets.

Thennakoon et al. developed a model that describes four different predictive patterns of fraudulent and past-identified activities[9]. When a suspicious transaction is performed with an API module that is informed through analytics and end-users, a warning is issued and this suspicious transaction is detected as fraudulent. In real-time applications, four different types of fraud have been identified with resampling techniques. The success of the proposed model was evaluated with support vector machines and Naive Bayes methods.

In recent years, the rapid development of e-commerce technologies, the desire of people to access every store and every product from all over the world in terms of price and quality makes life easier and offers various opportunities to fraudsters. Since credit card is the most popular payment method, fraudulent activities using credit card payment technologies are increasing rapidly. For this reason, in another study, credit card fraud detection was carried out by using traditional statistical methods and machine learning methods [10]. In this study, deep recurrent neural networks and ensemble model (ensemble methods) performed on two different datasets are proposed. Also, time analysis of the proposed model has been done and it shows that it is more efficient in real time. However, real-time detection and short-term fraudulent transactions, which are an important problem in detecting credit card fraud, did not yield very successful results.

Detection of credit card fraud is an important process of identifying fraudulent transactions before they occur. Adequate detection of fraud is very important for individuals and financial institutions. A hybrid study with various machine learning algorithms made by Kim was carried out for this purpose. It has also been compared with the proposed hybrid deep learning methods [11]. It offers a learning-based approach to the credit card fraud detection problem with a deep community method. They explained the effects of developing a hybrid community model and a deep learning model on credit card fraud detection. The most appropriate criteria for the performance measurement of the model are discussed.

III. Method

Artificial neural networks are generally used in the following areas. These; Animation, Simulation, Optimization, Virtual Reality, Cyber Security, Social Media, Entertainment Sector, Production/Consumption Sector, Marketing, Engineering, Industry, Health Sector, Finance, Communication, Security, Sports, Defense, Physics, Chemistry, Mathematics, Geography, Aviation, Military, Banking, Advertising, Education, Robotics, Control, Insurance, E-commerce, Automotive Sector, Space Industry [12].

Artificial neural network is one of the most important methods of artificial intelligence. Artificial intelligence is the development and analysis of intelligence in the machine. In recent years, many studies have been carried out with artificial neural networks. It has given very successful results, especially in solving complex and nonlinear problems[13].

The nervous system consists of nerve cells called neurons and the connections between them. Each of these connections is called a synapse. Neurons are the basic units of the nervous system and communicate with each other through these connections between them. The flow of information between neurons occurs through these connections. Each connection allows one neuron to send or receive a message to another neuron or to a body tissue [14].

ANN models usually consist of more than one layer. Except for the input layer, there are many neurons in each layer [15]. The neurons of each layer are parallel among themselves, while the neurons of the previous or next layer are in series. Since the neurons of each layer will send information to the next layer, there are connections between them. Since the output layer is the last layer, the connections end here. These links are represented by weights.

Weights are optimized during the learning process using training data. At the end of the training, it is tested whether the ANN model has learned by using the test data. Validation data, like a kind of test data, is used to test whether the ANN model has memorized or not during training. When the ANN starts to memorize the model, the training is stopped. However, the first place where memorization begins is referenced. If there is no memorization, the last iteration is referenced. If the learning has been achieved to a great extent, that is, the learning rate is no longer increasing, there is no need to continue education. Weight values in the reference iteration are used for test data [16].

While neurons at the same level do not affect each other, neurons used in successive layers affect each other [17]. Using more neurons at the same level increases the amount of information held in the network, while using successive layers increases the level of learning. However, there is an optimum point in the number of neurons and layers, continuously increasing the learning level does not increase continuously. However, it increases the computational load. Layer and number of neurons are hyper parameters that should be considered when creating a model. Using too many layers will increase both computational overhead and computational errors, as updating weights is done backwards.

The purpose of the tutorial is to find the weight values that will produce the correct outputs for the examples shown to the network [18]. Achieving the correct weight values of the network means gaining the ability to make generalizations about the problem represented by the examples. The process of achieving this generalization ability of the network is called network learning. The ANN model constantly updates the weights with the back propagation algorithm to minimize the difference between the real outputs and the calculated outputs during training.

The samples used to optimize the weights during the training are called the training set, and the samples used to test the success of the network at the end of the training are called the test set. The test set can also be used to see if the ANN model is actually learning, not to update the weights during training [19]. In this case, the test set is also the validation set. If it is desired to use a separate validation set, it is also appropriate to divide the entire data into three parts, approximately 70 percent training, 15 percent testing, and 15 percent validation sets.

In order to understand whether the training set used in the ANN model is sufficient, it is necessary to increase the number of data in the training set and see if the learning success of the network increases. However, this is not possible in the absence of a lot of data. In this case, the fact that the performances of the ANN model on the training and test data are close to each other can be accepted as an indicator [20]. For testing, a test set consisting of data not used in the training set is used. The inputs in the test set are given to the network and the output value of the network is compared with the desired output value. The aim is to see if the network can make an adequate generalization. This network can be used if the desired success is achieved in the training and testing stages.

The general features of artificial neural networks can be listed as follows [21,22,23,24]:

They have the ability to learn.

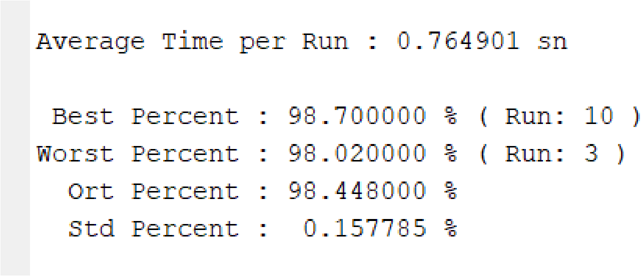
- They gain knowledge through learning.
- They learn by using examples.
- Learning takes place by training the network.
- They can learn with different learning algorithms.
- They learn by organizing themselves.
- By learning the events, they make similar decisions in the face of similar events.
- Thanks to their generalization abilities, they can also produce meaningful answers for examples not used during training.
- If the training set represents the problem space well, that is, if the examples cover all aspects of the case, it will be easier for them to generalize. They show higher achievement.
- They have the capacity to learn, memorize and infer relationships between data.
- Problem solving success is quite high.
- Demonstrating the problem to the network is difficult, requires user experience.
- There is no specific rule in determining the appropriate network structure and parameter values.

- Random selection of initial weight values within an appropriate range is important. Threshold values are also weights. The threshold value of each neuron is initially set to 0.
- It is difficult to explain the behavior of the network, that is, to analyze the learning process.
- They are hardware dependent and perform machine learning.
- They have a parallel distributed structure consisting of simple processing elements.
- They are designed in layers. The number of layers and the number of neurons in each layer increases the computational load.
- The information is not stored in a database, but spread over the entire network.
- Information has distributed memory because it is stored in connections.
- The memory is allocated and spanned over the network. It is included.
- They derive their strength from their ability to generalize and perform parallel operations.
- They must be trained and then tested in order to work safely.
- Working styles do not resemble known programming methods.
- They do not show sudden deterioration, they show gradual deterioration.
- They can work with incomplete information and process abnormal data.
- They have fault tolerance. They can process parasitic data.
- They can be used in detection events.
- They use lots of variables and parameters.
- They do not guarantee the optimum solution. They produce acceptable solutions.
- They are widely used in solving problems that cannot be expressed with formulas.
- They can be used to solve problems that cannot be expressed mathematically and are difficult to solve by humans.
- They are widely used in solving problems that cannot be solved by traditional calculation methods.
- Since they can only work with numerical information, the problem needs to be digitized.
- They are easily used in nonlinear multivariate systems.
- There is no specific rule about when the training will end. The average error is checked.
- They are in the form of computer programs as software and electronic circuits as hardware.
- Although they are not programmed for a particular problem, they can learn to solve it.
- Information processing methods are different from traditional programming.
- They can be used in detection events.
- They can make pattern recognition, completion, association and improvement.
- Many problems such as estimation, prediction, optimization, classification and modelling produce successful results.

IV. Experimental Study

Artificial neural networks are examined in four parts as single-layer perceptrons, multi-layer perceptrons, feed-forward neural networks and feedback. In our study, feed forward artificial neural networks are used, and all information transmitted in feed forward artificial neural networks moves from input to output. The neurons in one layer move towards the next layer and the correct information is transferred to the output layer.

The dataset we used in our study includes 284,807 transactions made with credit cards in September 2013 in Europe. The dataset consists of 28 inputs and 1 output. Our output includes 2 classes of 0 and 1, with or without credit card fraud. After the program.m file is run and the training process is completed, the result.m file is run. Figure 1 shows the accuracy results with feedforward neural networks for the credit card dataset. Here, the information of the best obtained value is available in the result. In the 10th run, the best value was reached and 98.70% value was achieved. The worst value was obtained in the 3rd run, and the value of 98.02% was obtained. Its mean value is 98.44% while its standard deviation is 0.15. It takes 0.76 seconds between each run.

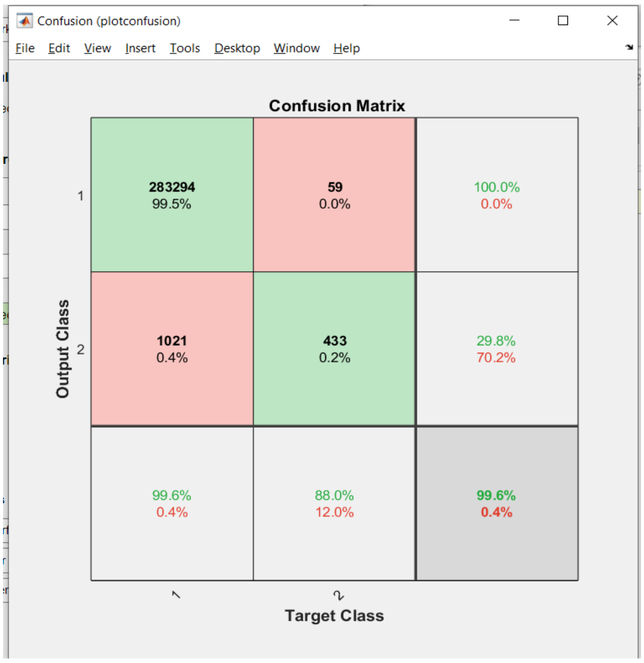


```
Average Time per Run : 0.764901 sn

 Best Percent : 98.700000 % ( Run: 10 )
Worst Percent : 98.020000 % ( Run: 3 )
  Ort Percent : 98.448000 %
  Std Percent :  0.157785 %
```

Fig. 1 Accuracy results for credit card dataset

Confusion matrix for a total of 284,807 transactions made on credit cards is given in Figure 2, and the performance curve is given in Figure 3. The Confusion Matrix is a tabular display of the current state in the data set and the number of correct and incorrect predictions of our classification model. The predicted class and the actual class labels are shown by confusion matrix. In Figure 4, we have shown how we can evaluate the performance of our classification model with the ROC graph. ROC is a probability curve for different classes. A typical ROC curve has False Positive Ratio on the X-axis and True Positive Ratio on the Y-axis. As seen in the receiver diagram in Figure 4, the rate of detecting fraudulent transactions in credit card is quite successful. Looking at the results, it has been observed that all transactions made with credit cards give good results with feed forward artificial neural networks.


Confusion (plotconfusion)
File Edit View Insert Tools Desktop Window Help
Confusion Matrix
Output Class
Target Class

	1	2	
1	283294 99.5%	59 0.0%	100.0% 0.0%
2	1021 0.4%	433 0.2%	29.8% 70.2%
	99.6% 0.4%	88.0% 12.0%	99.6% 0.4%

Fig. 2 Confusion Matrix

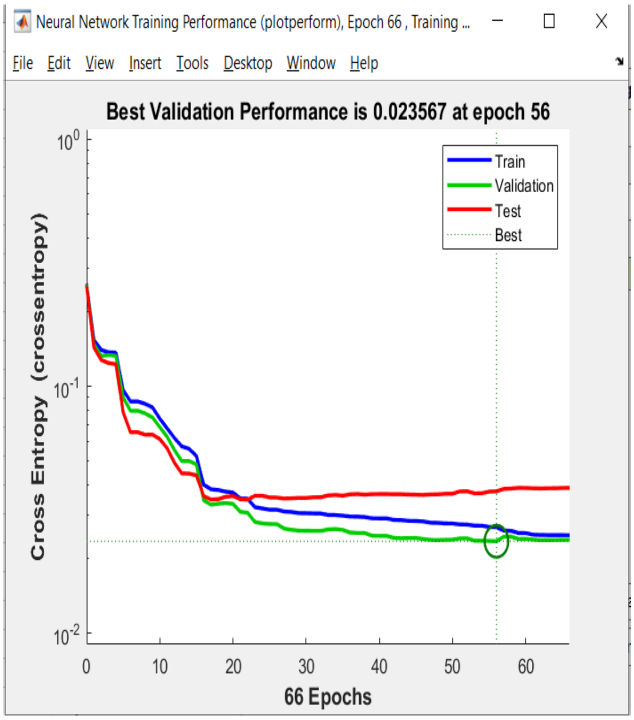


Fig. 3 Performance curve

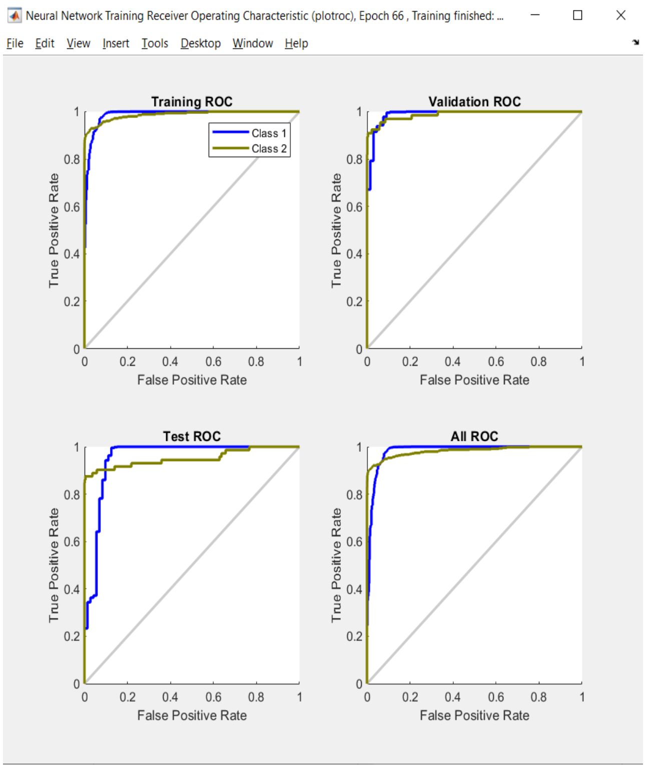


Fig. 4 Receiver diagram

V. Conclusion

With the development of technology, banking and financial institutions are also undergoing development and change day by day. Thanks to digital technologies, people perform their shopping, payments and expenditures with credit cards instead of using cash. In addition to these advantages, there are also some negative situations such as credit card fraud in the virtual environment that cause financial damage to people and harm people. These negative situations, which constitute a crime in terms of law and cause fraud, leave both individuals and different institutions such as banks in a difficult situation. In our study, we developed an automatic prediction model to detect credit card fraud in such cases. With the model we created with ANN, transactions that caused fraud in credit cards were detected with a success rate of 98.44%.

Acknowledgment

This article was created from Ferhat Yeşilyurt's master's thesis.

References

[1] Chen, J. I. Z., & Lai, K. L. (2021). Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence, 3(02), 101-112.

[2] Bhatt, A. N., & Shrivastava, N. (2022). Application of artificial neural network for internal combustion engines: a state of the art review. Archives of Computational Methods in Engineering, 29(2), 897-919.

[3] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit Card Fraud Detection using Machine Learning: A Study. arXiv preprint arXiv:2108.10005.

[4] Van Belle, R., Baesens, B., & De Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. Decision Support Systems, 164, 113866.

[5] Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. Mathematics, 10(13), 2272.

[6] Xie, Y., Liu, G., Yan, C., Jiang, C., Zhou, M., & Li, M. (2022). Learning transactional behavioral representations for credit card fraud detection. IEEE Transactions on Neural Networks and Learning Systems.

[7] Roseline, J. F., Naidu, G. B. S. R., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach☆. Computers and Electrical Engineering, 102, 108132.

[8] Alfaiz, N. S., & Fati, S. M. (2022). Enhanced Credit Card Fraud Detection Model Using Machine Learning. Electronics, 11(4), 662.

[9] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019, January). Real-time credit card fraud detection using machine learning. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488-493). IEEE.

[10] Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99, 106883.

[11] Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S. K., ... & Kim, J. I. (2019). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. Expert Systems with Applications, 128, 214-224.

[12] Sudheer, K. P., Gosain, A. K., Mohana Rangan, D., & Saheb, S. M. (2002). Modelling evaporation using an artificial neural network algorithm. Hydrological Processes, 16(16), 3189-3202.

[13] Philemon, M. D., Ismail, Z., & Dare, J. (2019). A review of epidemic forecasting using artificial neural networks. Epidemiology and Health System Journal, 6(3), 132-143.

[14] Wang, X., Lin, X., & Dang, X. (2020). Supervised learning in spiking neural networks: A review of algorithms and evaluations. Neural Networks, 125, 258-280.

[15] Cinar, A. C. (2020). Training feed-forward multi-layer perceptron artificial neural networks with a tree-seed algorithm. Arabian Journal for Science and Engineering, 45(12), 10915-10938.

[16] Ancona, M., Oztireli, C., & Gross, M. (2019, May). Explaining deep neural networks with a polynomial time algorithm for shapley value approximation. In International Conference on Machine Learning (pp. 272-281). PMLR.

[17] Dybkowski, M., & Klimkowski, K. (2019). Artificial neural network application for current sensors fault detection in the vector controlled induction motor drive. Sensors, 19(3), 571.

[18] Mumali, F. (2022). Artificial neural network-based decision support systems in manufacturing processes: A systematic literature review. Computers & Industrial Engineering, 107964.

[19] Indira, D. N. V. S. L. S., Ganiya, R. K., Ashok Babu, P., Xavier, J., Kavisankar, L., Hemalatha, S., ... & Yeshitla, A. (2022). Improved artificial neural network with state order dataset estimation for brain cancer cell diagnosis. BioMed Research International, 2022.

[20] Krenker, A., Bešter, J., & Kos, A. (2011). Introduction to the artificial neural networks. Artificial Neural Networks: Methodological Advances and Biomedical Applications. InTech, 1-18.

[21] Jain, A. K., Mao, J., & Mohiuddin, K. M. (1996). Artificial neural networks: A tutorial. Computer, 29(3), 31-44.

[22] Zhang, Z., & Zhang, Z. (2018). Artificial neural network. Multivariate time series analysis in climate and environmental research, 1-35.

[23] Dongare, A. D., Kharde, R. R., & Kachare, A. D. (2012). Introduction to artificial neural network. International Journal of Engineering and Innovative Technology (IJEIT), 2(1), 189-194.

[24] Zou, J., Han, Y., & So, S. S. (2009). Overview of artificial neural networks. Artificial neural networks: methods and applications, 14-22.