International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comparative Study on Machine Learning and Fuzzy Logic-Based Approach for Enhancing Credit Card Fraud Detection

Jayanthi. G[1], Deepthi. P[2], B. Nageswara Rao[3], M. Bharathiraja[4], Logapriya. A[5]

Submitted: 17/11/2023 **Revised:** 29/12/2023 **Accepted:** 09/01/2024

Abstract*:* The present research evaluates the efficacy of several machine learning models in credit card fraud detection, employing data sets of 284,407 transactions produced from online platforms. Careful data processing includes cleansing, scaling, mechanical properties, data imbalance management, and transient characteristics After preprocessing, five models— Artificial Neural Network (ANN), Support Vector Machine (SVM), Random were trained Forest (RF), Decision Tree (DT), and Naive Bayes (NB)—were assessed. Notably, ANN demonstrated an amazing performance of 97.6% accuracy, followed closely by SVM 95.5%, RF 94.5%, DT 92.3%, and NB 88.9% with the confusion matrices indicating high accuracy, true negatives, false positives, and false positives of each sample. It also gave little insight into the capacity to effectively identify false negatives. While ANN exhibited a very accurate, balanced detection of fraudulent and valid transactions, DT-NB showed a number of misclassifications rising disclosure. These arise from careful selection of machine learning models for credit card fraud detection, micro -And underline the significance of integration, with factors such as accuracy, translation, computational economy, and the etc. included. The study offers the standards and principles required to construct powerful and comprehensive credit card fraud detection systems, leading to gains in financial security and continually improving fraud prevention tactics.

Keywords: *Credit card fraud detection, Machine learning models, Artificial neural network, Support vector machine, Random Forest*

1. Introduction

Credit card theft has end up a huge issue in brand new virtual ecosystem, leading to severe economic losses for persons and organisations alike [1]–[4]. Because machine learning algorithms may rapidly and reliably produce fraudulent actions, there has been much interest on their effectiveness in treating this prevalent issue. This research intends to analyse the efficacy of machine learning algorithms in identifying and confirming credit scorecard fraud.

This research includes substantial data on 284,407 firms acquired from internet sources. The data set comprises of preparatory activities such as feature engineering, features scaling, data cleaning, usage of skewed data, and calculation of time These preprocessing techniques—neural network (ANN), support vector machine (SVM), random forest (RF), decision tree (DT), and naïve edge (NB)-for the optimization of the training data collection and assessment of the learning curve process.

The study results indicate the necessity for early development of banking systems for credit card fraud detection systems. Various components, which includes accuracy, interpretability, and computing performance, have to be taken into account at the same time as constructing robust and accurate fraud detection structures [8]–[11]. The study gives essential benchmarks and concerns for creating successful credit card fraud detection structures, leading to advances in economic protection and the continued growth of fraud prevention approaches. Credit card fraud is a prevalent issue that effects people, corporations, and financial institutions abroad. With the expanding digitalization of monetary transactions, fraudulent sports have emerge as additional state-of-the-art and challenging to discover employing traditional rule-primarily based structures [12]- [14]. Consequently, the usefulness of gadget learning procedures has surfaced as a potential technique to combat credit card fraud owing to their ability to examine enormous quantities of data, find difficult patterns, and create precise forecasts in real-time.

Previous researches have proved the efficiency of machine studying models in credit card fraud detection. One take a look at employed an ensemble of system gaining knowledge of methods, including decision trees, random forests, and gradient boosting, to obtain excessive accuracy in fraud detection. Their study underlined the necessity of feature engineering and facts preparation methodologies in increasing version performance [15]–[18]. Similarly, some other research applied deep gaining knowledge of strategies, principally convolutional neural

[1] *Associate Professor,
Department of Computer Science and Engineering (IoT),
Saveetha Engineering College, Chennai
Email: jayanthigovindaraju2015@gmail.com
ORCID: 0009-0000-0076-5175*
[2] *Assistant Professor, Department of CSE,
Madanapalle Institute of Technology & Science, Kadiri Road
Angallu Madanapalle, Andhrapradesh, 517325,
Email: deepthip@mits.ac.in
ORCID: 0009-0001-2072-1142*
[3] *Faculty of Mathematics, School of Technology, Apollo University
Murukambathu, Chittooru (Dist), A.p, India, Pin: 517127
Email: bendi151977@gmail.com, nageswararao_b@Apollo
university.edu.in
ORCID: 0000-0002-9197-5799*
[4] *Professor, Automobile Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, Erode
Email: bharathiraja@bitsathy.ac.in
ORCID: 0000-0003-1021-1840*
[5] *Assistant professor, Artificial Intelligence and Data Science
Panimalar Engineering College, Chennai
Email: logapriyaaruna@gmail.com
ORCID: 0009-0000-6235-2931*

networks (CNNs), to strike upon credit card fraud. The CNN version exhibited top notch accuracy and surpassed traditional gadget mastering models in recognising fraudulent transactions. The authors underlined the need of deep obtaining knowledge about models' capacity to automatically evaluate complicated patterns and respond to emerging deception techniques [19], [20].

These study, coupled with numerous others, illustrate the capacity of ML model models in credit score card fraud detection [21]- [23]. However, there's a need for future study to examine the performance of various system accumulating knowledge about algorithms and their applicability for actual-world applications. This modern-day look at aims to deal with this studies gap with the aid of comparing and analysing the overall effectiveness of five famous system learning models in credit card fraud detection, giving valued insights for the building of strong and accurate fraud detection systems [7], [24], [25].

The exploitation of system gaining knowledge of model presents top notch potential for credit score card fraud identification. This study adds to the existing frame of expertise by offering a full examination of distinct system acquiring knowledge of algorithms and their overall efficacy in identifying fraudulent transactions [5],[6],[26]. The facts of this research will resource within the development of improved fraud detection structures that could efficaciously lessen financial losses and boost monetary safety for folks and organisations.

2. Methodology

The primary motivation for this review is the fundamental need for better detection and prevention of credit card fraud. As the use of credit cards in online transactions increases, so does the risk of fraudulent activity. The consequences of credit card fraud extend beyond lost revenue, affecting individuals and financial institutions alike. A robust and accurate system for detecting fraudulent transactions is therefore essential to protect the interests of cardholders and financial institutions. The credit card fraud case used in this study was obtained from various online forums, which included information such as card number, account information, transaction details, datetime stamp, device information, type of transaction, fraud indicators and so on together, whereby many of machine learning models are built on the basis of training and research.

To improve credit card fraud detection, machine learning algorithms were trained using the aforementioned datasets. The training program involved the destruction of samples in terms of patterns and features of both normal and deceptive behavior. The diversity of data sets, including data sources, contributes to the flexibility and robustness of the model in identifying different fraud scenarios.

After the training phase, the models were rigorously tested to assess their accuracy in discriminating between real and deceptive interactions. The goal is not only to identify fraudulent information but also to identify potential fraudsters. Using machine learning models, this research aims to provide a sophisticated and automated approach to fraud detection, enabling financial institutions and companies to quickly identify suspicious activities and standardized and countermeasures.

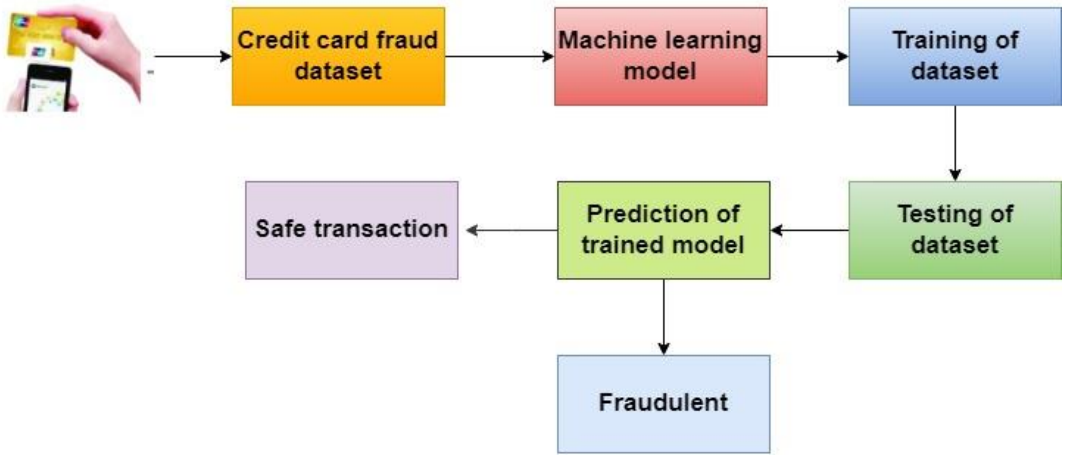

Fig. 1. Architecture of the proposed system

2.1 Preprocessing of dataset

In this study, 5 key extraction techniques have been performed to improve credit card fraud detection. It began off with extensive facts education, addressing deficient information, eliminating duplicates, and recognising redundancies. Feature scaling ensured that the numbers have been standardized, although function engineering offered additional variables. Data imbalance problems were alleviated using procedures inclusive of oversampling and undersampling. Temporal measures encompass time-dependent distributions and non-stop evidence of changing deception tendencies across time. Together, those tactics increased the dataset, letting system getting to know models to find difficult designs and helping to better pick out credit score card fraud that could be a lot one motive force of economic transactions.

Data cleansing is a critical phase within the research approach to ensure the integrity and dependability of the information employed to train machine studying models in credit score card fraud detection. This time with a crucial effort to handle appropriately with insufficient values. Methods which involves installing or putting off entries with inadequate information have been used to test the integrity of the dataset. To stay away from repetition, reproduction facts have been recognised and deleted, and continuous facts collection became developed for in addition investigations. Additionally, it became vital to come across and eliminate outliers to cope with unusual data points that may have an influence on the general performance of the models. By making use of these data purification strategies, the research intends to establish a robust base for subsequent feature extraction and model training.

Feature calibration is necessary to verify that statistical factors upload correctness to machine learning designs. In this study, standardization came into used to transform numeric components into standardized values, typically the employment of the z-rating normalising procedure. This strategy eliminates positive features from dominating the version training segment related to inequalities in length. By altering the qualities, models become more robust and less subject to fluctuations in characteristic length, thus enabling sample identification and accurate prediction in credit card fraud detection conditions is successful.

Feature engineering incorporates the inclusion of current, informative variables to enhance the discriminatory energy of system accumulating knowledge of models. In the area of credit score card fraud detection, these study presented new characteristics drawn from current ones. For example, transaction frequency, estimated by monitoring the time intervals of transactions, provided insights into customer activity patterns. Other developed functionalities were typical transaction amounts and time since the remaining transaction. These modifications targeted to gather subtle variables of credit card activity, enabling the models to research more efficaciously and make informed selections in figuring out possible fraudulent actions.

Addressing class imbalances in credit card fraud data sets is critical to avoid models from looking at the majority group (suitable function) A number of strategies were utilised in this research to balance the of the data kinds. Minority class oversampling (fraudulent interaction) and majority class undersampling were utilised to guarantee that the models met a more uniform representation of both classes throughout training. By lowering class imbalances, the models become more skilled at the subtle patterns associated with deceitful communication.

Temporal measurements play an essential part in credit card fraud detection, since fraudulent activity may display a temporal pattern or occur over time. The research includes temporal segmentation that analysed behavior across a certain period of time, such as days or weeks in. This method allowed the identification of temporal trends and changes in fraud tendencies. Additionally, rolling data were employed to record dynamic changes in characteristics over time, giving a complete insight of trending behaviors Considering temporal components, machine learning models were extremely responsive to the dynamics of credit card fraud, boosted their prediction powers and helped identify fraud more effectively.

Table 1. Preprocessing Steps

Preprocessing Steps	**Description**
Data Cleaning	Addressed missing values through imputation, removed duplicates, and identified and handled outliers.
Feature Scaling	Standardized numerical features using z-score normalization for uniform contributions to machine learning models.
Feature Engineering	Introduced new features, including transaction frequency, average amounts, and time-based metrics, to enhance model learning and discriminatory power.
Handling Imbalanced Data	Mitigated class imbalance through oversampling (fraudulent transactions) and undersampling (legitimate transactions).
Temporal Considerations	Segmented data based on time intervals and applied rolling statistics to capture temporal patterns and changes in features over time.

2.2 Machine learning model

In study articles that allow fraud detection, a variety of machine learning models were utilised, such as Naive Bayes (NB), Support Vector Machine (SVM), Artificial Neural Network (ANN), Decision Tree (DT), and Random Forest (RF). 30% of the dataset was set aside for testing the as-is, while the remaining 70% was utilised for training.

In this research, the Navie Bayes (NB) algorithm appears as a significant gadget research paradigm. NB is a probabilistic sort of approach based on Bayes' theorem, which employs conditional probabilities to produce predictions. Specifically, in the case of credit card fraud detection, NB operates by assessing the likelihood of fraud in a specific transaction. The "naïve" assumption of independence exposes power across types helps the calculation of probability, allowing for green schooling and prediction. This methodology has proved especially useful in handling complex and frequently restricted credit score card transaction details. During the training phase, NB studied the patterns in the dataset, learning to incorporate unique attribute combinations with possible fraud. The simplicity of versioning and speed of education and prediction phases makes it completely appropriate for huge datasets, which adds to the rational implementation in real-time fraud detection events Furthermore, analyzes for n' strengths and constraints are lighter in the area of credit scorecard fraud detection. The overall performance of the NB model was examined throughout the research. The insights gathered during the installation of the NB version offered vital assistance for the larger objective of establishing strong and reliable fraud detection systems as they emerge the overall usefulness of the study outputs has increased.

In this research, the Decision Tree (DT) algorithm played a vital role in detecting patterns in the data set. DT works by repeatedly splitting data based on attributes, generating a tree-like structure in which each node represents an attribute, each branch represents a decision based on that attribute, and a leaf node each has repercussions, in this example, whether prosecution is fair or deceitful. The sample architecture of the decision tree is shown in figure 2. The decision procedure comprises analysing the attributes of each node and identifying the appropriate separation that maximizes the resultant subgroups. Simple DT and interpretation make it beneficial for understanding the application of decision logic role in fraud detection. By evaluating the structure of the DT, the researchers acquired knowledge into the most significant criteria for identifying fraudulent activity. But the problem of overcomposition, when models recall training material and perform badly on fresh data, was addressed by approaches such as spinning. This research studied minor relationships between decision node components and outcomes under DT internally, a substantial link has been found in credit card transaction case studies its usefulness in collecting the results led to understanding the strengths and limits of DT considerably reduced credit card fraud detection, suggesting a larger objective of establishing a strong and reliable fraud detection method.

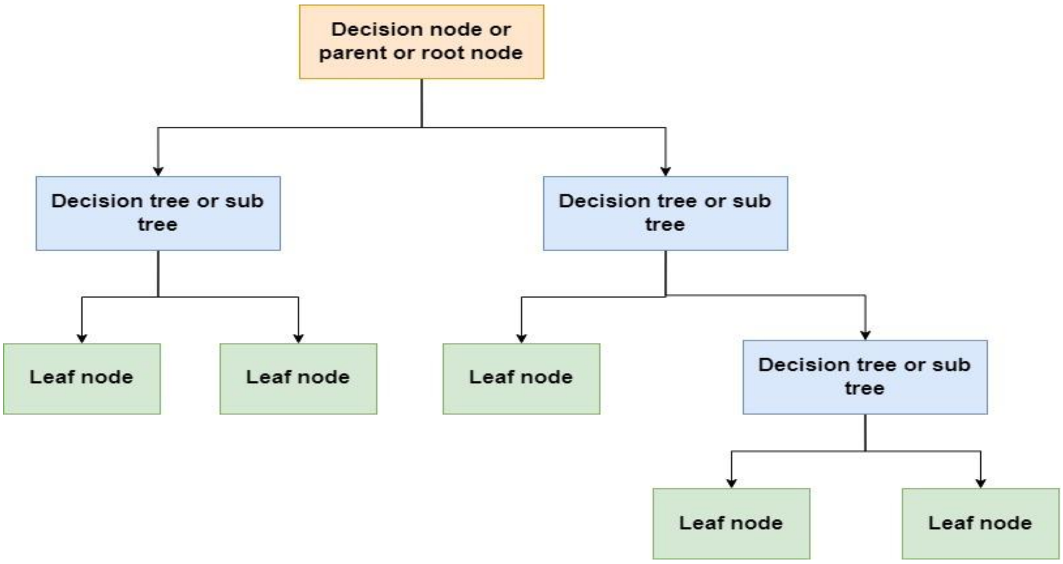
Decision node or parent or root node
Decision tree or sub tree
Decision tree or sub tree
Leaf node
Leaf node
Leaf node
Decision tree or sub tree
Leaf node
Leaf node

Fig. 2. Decision tree architecture

In the research, support vector machine (SVM) algorithms emerged as a powerful tool for classification tasks SVM performs by creating a hyperplane in multidimensional space separating data points well into classes. In fraud detection, the goal of SVM is to find a hyperplane that will maximize the distinction between legitimate fraudulent links, thus increasing the ability to generalize to unseen data Kernel tricks SVM can change basic feature the space, has enabled algorithms to capture complex relationships, which are not linear in content. This study investigated the performance of SVM, as it identifies an optimal hyperplane and classifies actions based on their position along these boundaries. The concept of a support vector representing important data points for defining hyperplanes was used especially in understanding SVM decisions. The study provided useful insight into the effectiveness of algorithms under complex patterns within credit card transaction data. The findings contributed to a nuanced understanding of the strengths and limitations of SVMs, and happens highlighting the ultimate goal of developing sophisticated and accurate credit card fraud detection systems.

In this investigation, the random wooded area (RF) strategy proven to be a reliable and flexible machine getting to know version for identifying credit card fraud. It concluded effective estimates by means of applying many RF timbers with superb decision trees, taking into consideration the aggregate power utilisation. Every individual tree in the woods is skilled on a certain component of the knowledge. When creating forecasts, the implications from each tree are aggregated via balloting or averaging. This clustering strategy not most effective mitigates the issue of overfitting, although it boosts the model's ability to realise sophisticated institutions internal credit card transaction facts. Random Forest (RF) comprises of randomization by randomly picking and bagging a subset of features for every tree. This system is regulated by bootstrap sampling. This stochasticity boosts the adaptability and flexibility of the version, making it particularly green in solving complex fraud detection situations. The investigations extensively examined the internal working of the RF, clarifying how the amalgamation of numerous decision trees affects in a robust and distinctive fraud detection framework. The studies investigated the significance of prioritisation in RF (radio frequency) and emphasized the important thing elements that effect the categorization of offerings as both true or deceptive in RF overall performance evaluation, which in flip impacts the effectiveness of latest gadget getting to know algorithms. Performing an examination to recognise patterns and irregularities in credit card transaction data. The full evaluation of the RF, which provided large insights into its usefulness in criminal court cases, increased refined grasp of its skills and limitations, arranging it as a vital resource for better and reliable credit score card fraud detection structures.

Artificial neural networks (ANN) have been applied as a successful and breakthrough system getting to know approach within the investigation of credit score card fraud detection on these studies. ANNs are inspired by means of the complicated design of the human brain, with interconnecting hidden and output layers as shown in figure 3. Each combination of nodes is connected with a weight, and throughout training, this weight is changed to minimize the discrepancy between expected and actual outcomes. For credit card fraud detection, input the layer represents things like transaction information, while the output layer offers segmented findings. The activation function used to the weighted sum of inputs at each node generates nonlinearity, allowing the network to record complicated patterns. The work explained the ANN training procedure for forward and backward propagation. In forward propagation, the input data is transferred through the network, creating predictions. The backpropagation then modifies the background weights depending on the prediction error, boosting the generalizability of the network. ANN algorithms, to model complicated interactions, and optimize diverse financial models, to identify credit card fraud. The regular ability research evaluated the influence of network architecture, such as number of layers and neurons, on performance, ANN showed excellent results bae. Provided insights about its correct design through a detailed review of ANN performance, this work has contributed to nuanced understandings of its strengths and contextual constraints.

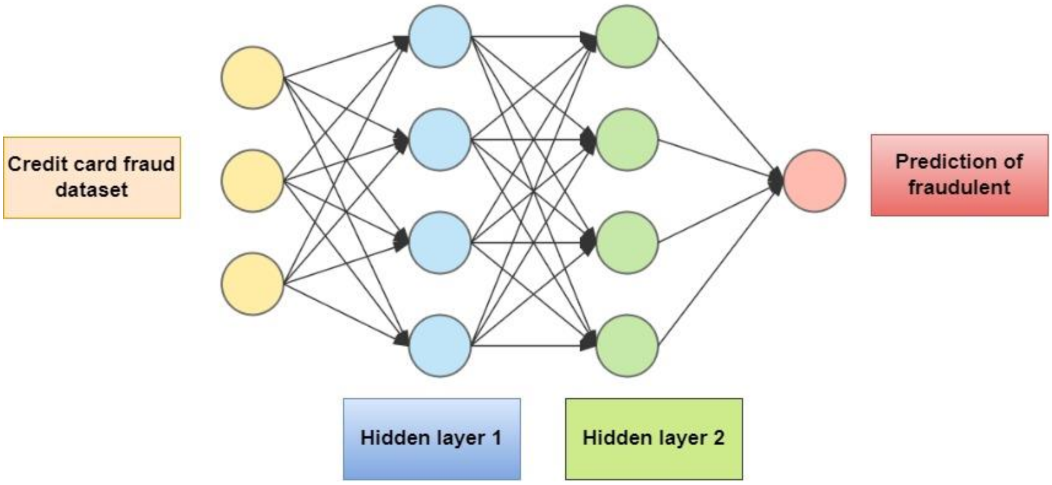

Fig. 3. ANN Model Architecture

3. Result and Discussion

Following the training process for each machine learning model in this study, the suggested technique underwent rigorous testing to assess its performance in credit card fraud detection. The findings indicated substantial performance variances across the models. The accuracy of the each model are shown in figure 4. The Artificial Neural Network (ANN) exhibited the best predicted accuracy, earning an amazing 97.6%. SVM closely followed with a remarkable accuracy of 95.5%, while the Random Forest (RF) and Decision Tree (DT) models attained accuracies of 94.5% and 92.3%, respectively. The Naive Bayes (NB) model revealed a decent accuracy of 88.9%. These results emphasised the usefulness of the suggested strategy, notably showing the improved performance of the ANN model in properly recognising fraudulent transactions.

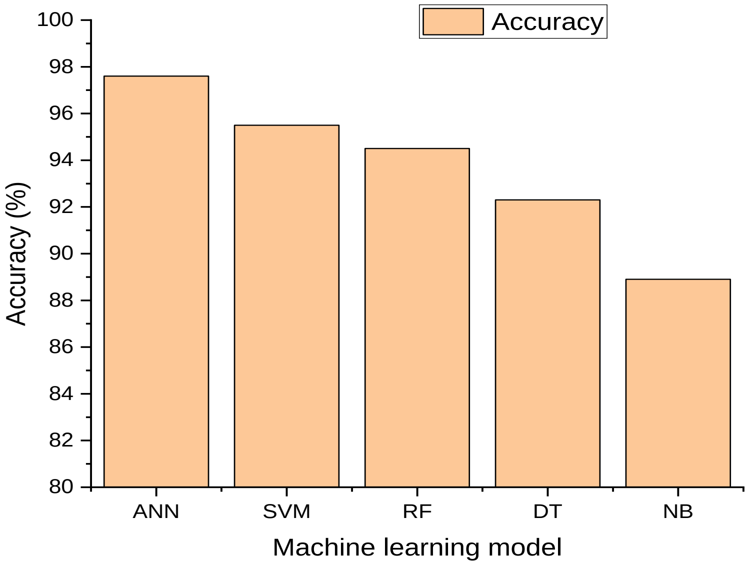

Fig. 4. Accuracy of each model

Performance Analysis Figure 5 highlights the efficacy of each machine learning method employed in credit card fraud detection study. Precision measures the overall accuracy of the forecasts, whereas accuracy shows how effectively the model can identify fraud instances within the positive predictions Recall assesses the model's capacity to catch all real fraud, and F1 score balances accuracy with in the memory. The table reveals that the Artificial Neural Network (ANN) beats the other models with an accuracy of 97.6%, which displays its unique ability in classifying tasks correctly followed closely by Support Vector Machine (SVM) with 95.5%, and very great performance has been proved. The figure 5 gives a complete comparison of important performance parameters, allowing analysts identify the best suited model for their credit card fraud detection system.

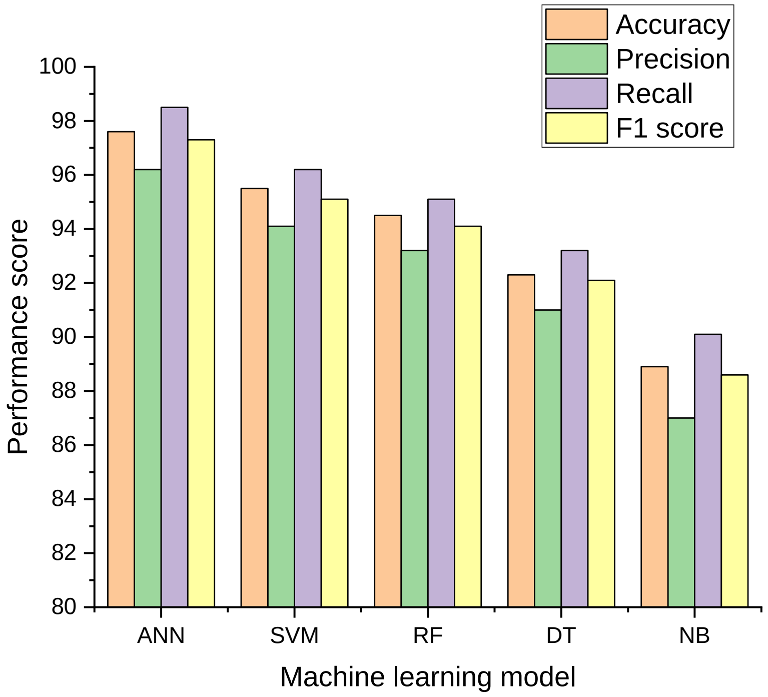

Fig. 5. Performance score of each machine learning model

Each machine learning model for credit card fraud detection analysis is represented by a confusion matrix, which is shown in Figure 6. A true positive (TP) implies successfully discovered deceptions, whereas a true negative (TN) reflects the best categorization of related jobs. False positives (FP) relate to genuine usage that have been misdiagnosed as fraudulent, whereas false negatives (FN) refer to fraudulent uses that have been misclassified as valid Notably, artificial neural network (ANN) scored 7,850 TPs and 18,850 TNs, compared to fraud . Support Vector Machine (SVM) and Random Forest (RF) demonstrated efficient efficiency in balancing between TP and TN and also displayed strong observable characteristics. Decision tree (DT) and naïve Bayes (NB) models, although displaying robustness, demonstrated significant rates of FN and FP, underlining the necessity to carefully evaluate the trade-off between accuracy and recall in model fit before any selection of Credit card fraud detection is proven. The extraordinary accuracy of the artificial neural network (ANN) of 97.6% exhibited excellent performance similar to vector machine (SVM) and random forest (RF) concentrating and performing well in equally distributed interactions, and exceeded the new models Decision Tree (DT) and Naive Bayes over (NB) models, although displaying reasonable accuracy, demonstrated considerable amounts of false negatives and false positives emphasising possible areas for improvement Such information these asset-linked systems bring substantial insights to the industry, enabling for complicated credit card fraud cheating Behind system detection, balancing accuracy and efficiency, concerns of model housing, computing complexity, and adaptability are major factors Wider applicability of this approach to real-world scenarios should be considered.

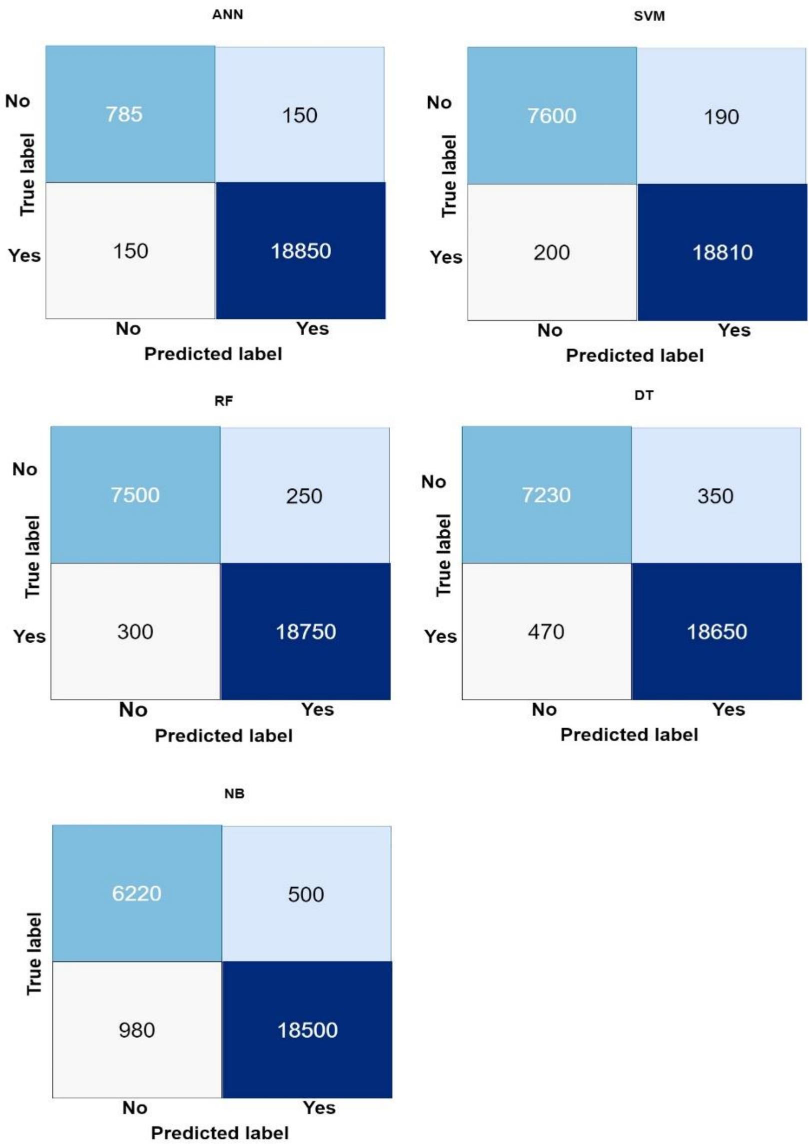

Fig. 6. Confusion matrices of each model

4. Conclusion

In conclusion, this research represents a comprehensive review of machine learning models for credit card fraud detection. Using a combination of data from various online platforms, the study carefully applied a variety of preprocessing techniques, including data washing, measurement, processing, data imbalance handling, and reasoning were used in the analysis including five main paradigms: Artificial Neural Networks (ANN). Support Vector Machine (SVM), Random Forest (RF), Decision Tree (DT), and Naive Bayes (NB) Surprisingly, the ANN model emerged as the leading candidate, achieving an impressive accuracy of 97.6%, showing a superior ability to accurately discriminate deceptive behaviors followed closely by SVM and RF, which showed strong performance at 95.5% and 94.5% accuracy, respectively. The decision tree and naive Bayes models exhibited limitations in terms of false positives and false negatives even though they exhibited respectable accuracies of 92.3% and 88.9%. Subtle insights from the confusion matrices occurred further emphasize that each sample is given a genetic trade-off between accuracy and memory. These factors assist drive the design and development of models depending on certain goals, such as the necessity of effectively identifying fraudulent interactions or lowering false positives. Additionally, the study gives useful insights to academics and practitioners in credit card fraud detection, offering insights into the strengths and possible areas for development of different machine learning approaches. Besides adding to learning discourse, these measurements have practical relevance Strengthen financial security in a digitally linked world.

References

[1] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *Eurasip Journal on Information Security*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-00111-0.

[2] M. Preetha *et al.*, "Efficient Re-clustering with Novel Fuzzy Based Grey Wolf Optimization for Hotspot Issue Mitigation and Network Lifetime Enhancement," *Journal of Ad Hoc & Sensor Wireless Networks*, Vol. 56, Issue 4, page No-273-297, Sep 2023

[3] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, "Online payment fraud: from anomaly detection to risk management," *Financial Innovation*, vol. 9, no. 1, 2023, doi: 10.1186/s40854-023-00470-w.

[4] T. Zhu *et al.*, "RiskCog: Unobtrusive real-time user

authentication on mobile devices in the wild," *IEEE Transactions on Mobile Computing*, vol. 19, no. 2, pp. 466–483, 2020, doi: 10.1109/TMC.2019.2892440.

[5] H. Alam *et al.*, "IoT Based Smart Baby Monitoring System with Emotion Recognition Using Machine Learning," *Wireless Communications and Mobile Computing*, vol. 2023, 2023, doi: 10.1155/2023/1175450.

[6] S. Kyeong and J. Shin, "Two-stage credit scoring using Bayesian approach," *Journal of Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00665-5.

[7] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[8] J. Petch *et al.*, "Machine learning for detecting centre-level irregularities in randomized controlled trials: A pilot study," *Contemporary Clinical Trials*, vol. 122, no. September, p. 106963, 2022, doi: 10.1016/j.cct.2022.106963.

[9] Q. Zhao, K. Chen, T. Li, Y. Yang, and X. F. Wang, "Detecting telecommunication fraud by understanding the contents of a call," *Cybersecurity*, vol. 1, no. 1, pp. 1–12, 2018, doi: 10.1186/s42400-018-0008-5.

[10] M.Preetha *et al.*, "A Survey on Microcontroller based Machine to Machine Interaction with Temperature Control System", International Journal of Advance Engineering and Research Development (IJAERD), Vol.5, No 2, pg.159-162, February 2018. Print ISSN 2348 - 6406, Online ISSN 2348 – 4470

[11] M. E. Edge and P. R. Falcone Sampaio, "The design of FFML: A rule-based policy modelling language for proactive fraud management in financial data streams," *Expert Systems with Applications*, vol. 39, no. 11, pp. 9966–9985, 2012, doi: 10.1016/j.eswa.2012.01.143.

[12] I. Priyadarshini *et al.*, "A new enhanced cyber security framework for medical cyber physical systems," *Software-Intensive Cyber-Physical Systems*, vol. 35, no. 3–4, pp. 159–183, 2021, doi: 10.1007/s00450-021-00427-3.

[13] K. A. Alaghbari, M. H. M. Saad, A. Hussain, and M. R. Alam, "Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations," *Journal of Cloud Computing*, vol. 11, no. 1, 2022, doi: 10.1186/s13677-022-00338-x.

[14] Preetha M *et al.*, "A Survey on Entry Restriction System for the fake server Scheme", International journal of Research and Engineering (IJRE), Vol.4, No 2, pg.41-44, February 2017. ISSN:2348-7860(0).

[15] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications*, vol. 193, p. 116429, 2022, doi: 10.1016/j.eswa.2021.116429.

[16] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, 2022, doi: 10.1186/s40537-022-00573-8.

[17] M. Ala'raj, M. F. Abbod, and M. Majdalawieh, "Modelling customers credit card behaviour using bidirectional LSTM neural networks," *Journal of Big Data*, vol. 8, no. 1, 2021, doi: 10.1186/s40537-021-00461-7.

[18] M. Preetha *et al.*, "A Preliminary Analysis by using FCGA for Developing Low Power Neural Network Controller Autonomous Mobile Robot Navigation", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799

[19] Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," *Journal of Big Data*, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.

[20] R. M. Dantas, R. Firdaus, F. Jaleel, P. Neves Mata, M. N. Mata, and G. Li, "Systemic Acquired Critique of Credit Card Deception Exposure through Machine Learning," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 8, no. 4, 2022, doi: 10.3390/joitmc8040192.

[21] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 145–174, 2023, doi: 10.1016/j.jksuci.2022.11.008.

[22] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques," *Procedia Computer Science*, vol. 218, pp. 2575–2584, 2023, doi: 10.1016/j.procs.2023.01.231.

[23] M. Preetha *et al.*, "Deep Learning-Driven Real-Time Multimodal Healthcare Data Synthesis", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799, Vol.12, Issue 5, page No-360-369, 2024

[24] T. A. Olowookere and O. S. Adewale, "A framework for detecting credit card fraud with cost-sensitive meta-learning ensemble approach," *Scientific African*, vol. 8, p. e00464, 2020, doi: 10.1016/j.sciaf.2020.e00464.

[25] M. Habibpour, H. Gharoun, M. Mehdipour, and A. Tajally, "Engineering Applications of Artificial Intelligence Uncertainty-aware credit card fraud detection using deep learning," *Engineering Applications of Artificial Intelligence*, vol. 123, no. January, p. 106248, 2023, doi: 10.1016/j.engappai.2023.106248.

[26] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, no. December 2022, p. 100163, 2023, doi: 10.1016/j.dajour.2023.100163.