Volume 9, Issue 4, April – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

# Credit Card Fraud Detection System

Dhanashree Diwase[1]; Janhavi Warkari[2]; Abhishek Gawali[3]; Swati Shamkuwar[4]
[1,2,3,4] Department of Information Technology, G.H. Raisoni College of Engineering, Nagpur, India,

**Abstract:- Globally, credit card fraud is a serious threat to people, businesses, and financial institutions. With the rise of online transactions, fraudsters have developed clever ways to take advantage of loopholes in payment systems. Traditional fraud detection methods based on manual inspections and rules-based systems are unable to counteract this new and evolving risk. As a result, the use of data analytics and machine learning has become a viable option for real-time detection and prevention of credit card fraud. The paper looks at using machine learning algorithms such as logistic regression, decision trees, random forests, neural networks, etc. to detect fraudulent transactions We go over the importance of data sources and components, analytical metrics, and how fraud detection on the effectiveness of examples. In addition, we list the current challenges and directions in which credit card fraud detection is likely to continue, including the use of blockchain technology and sophisticated AI techniques. Overall, this study highlights the importance of credit card theft detection and the promise of machine learning in mitigating this ubiquitous problem financial institutions use advanced machine learning algorithms and analytics function to detect fraudulent behaviour, protect customer interests, and maintain payment environment integrity to improve their capabilities.**

***Keywords:-*** *Credit Card Fraud Detection, Machine Learning, Deep Learning, Anomaly Detection, Performance Metrics.*

## I. INTRODUCTION

Credit cards provide consumers and businesses with unmatched ease and flexibility in today's interconnected digital economy, helping to facilitate a wide range of transactions. But in addition to the advantages of using credit cards, there is a constant and widespread risk in the shape of credit card theft. Financial institutions, retailers, and cardholders throughout the world face serious difficulties because of this danger, which includes a variety of illegal activities such as identity theft, unauthorized transactions, and account takeover. Technology advancements and the growing popularity of online shopping have made credit card fraud even more complex by giving thieves access to more advanced methods for targeting weaknesses in the payment system.

These tactics consist of, but are not restricted to, point-of-sale terminal card skimming devices, scams attack at gullible customers, and advanced malware intended to steal cardholder information. Because of this, the financial sector constantly must fight to keep ahead of scammers and safeguard the integrity of the payment system.

The impact of credit card fraud is extensive and affects a wide range of people. The impact on financial institutions goes beyond lost revenue; They also face regulatory scrutiny and loss of their brand. Financing could be severely strained by the cost of reimbursing cardholders for fraudulent purchases, monitoring incidents, and putting fraud protection measures in place Again also, financial institutions risk fines and legal action if they fail to adequately protect customer data and stop fraud. Credit card fraud disproportionately affects merchants, costing them money in lost sales, penalty charges, and damaged consumer trust. Small businesses in particular may find it difficult to recover from the loss of revenue caused by fraudulent transactions, jeopardizing their sustainability and future growth opportunities. [1,2]

Also, merchants bear a disproportionate share of the cost of fraud prevention solutions such as PCI DSS compliance, EMV chip technology, which increases operational costs. Theft undermines consumer confidence in the security of electronic payments in , resulting in fewer people using their cards, more people switching to alternative payment methods In this context, protecting the interests of all parties involved and maintaining trust a maintained in the integrity of the payments ecosystem depends largely on effective fraud detection and prevention strategies.

## II. METHODS OF CREDIT CARD FRAUD DETECTION

- *Card Skimming*

The most common type of credit card fraud is called "card skimming," which consists of card skimming devices that are smuggled into popular card readers such as ATMs or point-of-sale terminals when a card is inserted for a transaction Name, account number, expiration date, and other sensitive information needed to secure the transaction are often included in the stolen data.[3] Fraudsters can then use this information to create fake cards or run illegal transactions, costing cardholders and financial institutions a lot of money scraping machines can be hard to detect because they can be incredibly tricky, blended seamlessly with the original card reader.

To further support the fraudulent activity, attackers can also use other techniques such as overlays or hidden cameras to record PINs. Dealers and consumers need to be extra careful about finding spinning machines. This requires

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

careful monitoring of card readers for any discrepancies or signs of tampering. Advanced security measures can help prevent card hacking attempts and protect cardholder information. These include non-destructive seals, periodic maintenance, and storage technologies. However, skimming techniques highlight how difficult it will always be to deal with this type of credit card fraud. [2,3]

➢ *Phishing*

Phishing is a type of cybercrime that involves fraudulent attempts to obtain personal information from people such as credit card numbers, usernames, passwords, etc. Usually heard through electronic messaging systems that instant messaging, SMS, and email use such efforts. Phishing is the practice of impersonating reputable companies or organizations—such as banks, social media platforms, Internet retailers, or government agencies—that a victim can trust social engineering techniques are often used use phishing attacks to lure victims into revealing private information or taking actions that threaten their security.

Sometimes, Phishing emails or messages contain creative or interesting requests, such as reporting an account security breach, requests to verify account information, offer incentives or rewards These messages can created links to a fake website that appears a lot. Sometimes the letters contain viruses or malicious software that, if detected, can infect the victim's computer with malware and infect the attacker gain access to the victim's device, allowing it to retrieve confidential data or access systems without confidentiality.

➢ *Phishing Attacks can Take Various Forms, Including:*

- Spear Phishing: Spear phishing is the term for targeted attacks that are aimed at certain people or companies. Personalized information is frequently used to make the phishing attempt seem more legitimate.
- Clone phishing: Clone phishing involves altering authentic emails or webpages and distributing them to victims under the false pretence of being authentic.
- Smishing: Phishing attacks carried out on mobile devices through text messaging (SMS) or multimedia messaging services (MMS).
- Vishing: Vishing is the term for phishing assaults over voice calls, in which con artists try to trick victims into divulging personal information.

➢ *Carding*

Carding is a very complex and elaborate form of credit card fraud involving many steps and processes. The process usually begins with the discovery of stolen credit card information. This can happen in a variety of ways, including data breaches, installation of scanning devices at ATMs or retail locations, phishing scams targeting specific people or businesses, or cards about stolen information purchased from so-called underground online "carding forums."

After fraudsters obtain credit card information through theft, they often perform "card checks" to confirm the authenticity of the data. To ensure that the credit card is active and not reported lost or stolen by the cardholder or bank, this includes using stolen credit card credentials for small transactions or lit purchases considered.

If the stolen credit card information passes half the test, fraudsters use the compromised credit card information to create a fake credit card. Stolen card information using magnetic tape writers or other card copying devices is often applied to blank or counterfeit cards throughout this process after which the counterfeit card imitates the cardholder real information and ready to be used for illegal transactions or withdrawal of funds.

Fraudsters use a variety of techniques to commit illegal acts through fake documents, such as purchases in physical locations, use of online trading platforms, advance withdrawals at ATMs or reducing the privilege of banking types or merchants will find it. Money laundering techniques are another tactic used by fraudsters from time to time. The proceeds of fraudulent transactions are used to launder money through various channels such as cryptocurrency exchanges, offshore bank accounts and shell corporations.

➢ *Card Not Present (CNP)*

Card Not Present (CNP) fraud is a common form of credit card fraud when a physical credit card is not presented during online or telephone transactions. Cybercriminals use a variety of methods to obtain credit card information, such as data breaches, phishing schemes, or purchasing stolen card numbers from shady Internet marketplaces called "carding platforms" Once this data is obtained a, this data is used—without the cardholder's knowledge—for illegal purchases. Because physical card verification is not involved, CNP fraud presents different detection and prevention issues than card-based transactions. However, red flags can indicate potential fraud. These may include unusually large transactions, shipments other than the billing address, or repeated denials of permit requests.

To reduce risk, financial institutions and merchants use fraud protection techniques such as address verification systems (AVS), card verification value (CVV) checks, 3D secure authentication and more to identify transactions which is immediately suspicious and the cardholder's name is confirmed -Recommend merchants to limit, and regularly review their credit-card accounts for fraud, Follow regulatory standards such as Payment Card Industry Data Security Standard (PCI DSS) background to protect cardholder data and stop CNP fraud. This underscores the need for those involved to work together in the fight against such fraud and to ensure that online communications are secure.

## III. TRADITIONAL FRAUD DETECTION METHODS

Traditional fraud detection methods obviously rely on transaction monitoring, manual search algorithms, and rule-based algorithms to detect fraudulent transactions. Rules-based systems identify projects that fall within established

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

policies, using predefined criteria or requirements, such as unusually large purchases or projects from high-risk areas. This method has little scalability and is prone to human error but is weak in detecting subtle deceptive behaviours. Real-time accounting system analysis is used by transaction monitoring systems to identify anomalies or systems indicative of fraud such as unusual spending Although these traditional methods have had some success, they have failed do not keep up with the rapid advances in fraud techniques.

- *Rule-Based Systems*

Traditional fraud detection techniques are based on rule-based systems, which use established criteria to identify possibly fraudulent transactions. These guidelines, which indicate transactions that depart from accepted patterns or behaviours, are based on past data, industry standards, and fraud tendencies. Rules could be established, for instance, to send out notifications if a certain dollar amount is transacted, a country is considered high-risk, or several transactions occur within a brief period of time. Although rule-based systems are easy to use and comprehend, they have the potential to produce false positives or identify emerging fraud trends that don't match pre-established rules. Because of this, ongoing rule modification and improvement are required to guarantee that rule-based fraud detection systems are effective in thwarting new threats and reducing false positives.

- *Manual Review*

In manual analysis to detect fraud, human analysts scrutinize flagged transactions for authenticity and identify potentially fraudulent information to determine the likelihood of fraudulent activity, analysts examine behaviour types such as purchase volume, frequency of transactions, geographical presence, and customer behaviour well patterns, such as accounting activity, customer history, In transaction-irregularities.

Investigations into transactions reported by financial institutions' suspicious activity reports or automated fraud detection systems are often the first step in the manual inspection process Then investigators use that ranks these flagged transactions according to risk criteria such as issue size, type, or customer profile. Reviewing high-risk behaviours is prioritized to prevent recurrences.

Investigators use various techniques and tools throughout the investigation process to confirm the authenticity of the transaction and detect any fraudulent activity These may include contacting customers directly to obtain confirmed information about their transaction, they will search suspicious persons or areas, and cross-reference with databases internal and external to the company To accomplish each, investigators may also work with other organizational departments, such as fraud investigation teams or the legislature.

Manual analysis has its drawbacks, although it provides valuable experience and valuable flexibility to uncover complex fraud patterns that automated systems can overlook If a large number of tasks are handled correctly manually the research process is highly demanding of manpower due to its labour-intensive and time-consuming nature.

- *Transaction Monitoring*

Transaction monitoring is an integral part of traditional fraud detection techniques to protect financial institutions and vendors from fraudulent practices It involves continuous, real-time transactional data with complex statistical modelling, planning, and analytics using predefined types to identify unique systems and features collects and analyses transaction data from a variety of sources, including online payment gateways, To identify potential indicators of fraud involving ATM networks and points of sale, the study looks at transaction volume, frequency, timing, locations and customer behaviour.

Behavioural analytics, which provides initial patterns of specific behaviour for certain customers or accounts, is one of the primary methods used in transaction tracking Additional analytical alerts can be triggered by deviating from any of these default settings so To identify patterns associated with policy This model, which also uses pattern recognition algorithms, can produce fast, expensive transactions followed by cash withdrawals, regular payments to organizations whose mentally impaired, or transactions consistent with established fraudulent patterns.

- *Customer Verification*

The process of customer care is more complex and important than traditional fraud detection methods. It focuses on confirming the legitimacy of the transaction and the identity of the cardholder. Address verification is a popular technique that compares a given billing address with information held by the issuing bank and identifies discrepancies as possible red flags Additionally, telephone verification is to contact the cardholder in person to verify the transaction details over the phone—either through a personal call or conversation with customer support staff. Authentication requires a variety of methods, including biometric verification—using fingerprint or facial recognition technology to verify authenticity—and knowledge-based authentication (KBA), which requires that respondents provide accurate answers to questions based on personal data.[11]

Verifying credentials such as a passport or driver's license requires two types of authentications a password and a one-time code factor authentication (2FA) for an email address or mobile devices Increases Security While these steps help prevent fraud, they do can complicate the customer experience and create a possibility to protect against more complex fraudulent schemes. Consequently, companies must constantly improve and optimize these processes to achieve a delicate balance between strong security measures and flawless user experiences.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

## IV. MACHINE LEARNING MODELS IN CREDIT CARD FRAUD DETECTION

➢ *Supervised Learning*

The first step in the supervised learning process for credit card fraud detection is to obtain representative datasets of past transactions identified as legitimate or fraudulent and to train and test devices learning models have looked like a basis for this dataset. Each transaction is typically accompanied by a wealth of information, including transaction cost, completion date, location, Merchant Class Code (MCC), and any other metadata such as device information or carrier use the character set.

To ensure data quality and accuracy, extensive data pre-processing procedures are carried out before the data is entered into the machine learning model This includes coding of categorical variables, monitoring for outliers, missing data if they will be filled in, along with scaling mathematical elements to match the normal scale. In addition, relevant data can be extracted, feature engineering and other techniques can be used to generate new features, which can improve the predictive capability of the model.[5]

Once the data set is prepared, several supervised learning algorithms are trained with the labeled behavioural data. Based on the patterns and relationships found in the data, each algorithm learns how to map the inputs to the corresponding binary label (fraud). To maximize its predictive power during training, the model repeatedly modifies its parameters to minimize the chosen loss function, such as hinge loss or cross-entropy loss.

After training, the ability of the model to generalize is tested by examining its performance on a different validation data set. Metrics including precision, accuracy, recall, F1-score, and area under the ROC curve are commonly used in these studies to measure model performance to further improve performance and optimize the hyper parameters and model architectures for refinement an unnecessary problem.

Proper performance on the authentication data set provides a pattern for real-time fraud detection. The model continually analyses transaction events in the manufacturing process, using the limited sample to classify each transaction as legitimate or fraudulent Additional research and training with newly labelled data is required and to keep the model running smoothly over time and to adapt to changing frauds.

Generally, supervised learning uses machine learning algorithms to detect fraudulent behaviour in the form of strategic data design, simulation training, analysis, and deployment in a capable manner reliability and effectiveness Organizations can use the predictive capabilities of supervised learning to improve their ability to detect fraud and mitigate financial fraud risk.

➢ *Unsupervised Learning*

In credit card fraud detection, unsupervised learning programs cover several different techniques, each with specific benefits and applications. By grouping tasks based on similarity, network clustering methods such as DBSCAN and k-means clustering make it possible to identify underlying features—networks that do not fall into any existing group Thus these irregularities, or outliers can be indicators of fraud and it needs to look closely. Clustering methods can be useful for identifying discrete features, but they cannot deal with complex or overlapping fraud patterns. The effectiveness of the clustering algorithm and parameter setting can also significantly influence the results.[5]

Another unsupervised learning method designed to detect anomalies in high-dimensional datasets, such as credit card transactions, is provided by splitting forests These forests are ideal for detecting anomalies in more obvious practices when information is repeatedly partitioned into smaller groups and outlying features are reduced in fewer divisions , single-class partitioning methods such as auto-encoders and support vector machines (SVM) learn to distinguish between anomalies and normal behavior based only on common instance attributes These models can detect deviations indicative of deceptive behavior because they are trained on data representing only normal so the behaviour is performed. This means that even in the absence of listed examples of fraud, meaningful assessments can be provided.

Furthermore, threshold-based approaches, in which specific thresholds are specified on behavior attributes or metrics, can also be used to detect undetected fraud, any behaviour beyond these thresholds is considered potentially distorting. Despite being easy to implement, threshold-based methods can have trouble setting precise thresholds, which provide a compromise between false positive reduction and fraud detection Furthermore, threshold-based systems embedded with advanced unsupervised learning techniques Need to be developed because subtle and complex deceptive functions of the extreme may be missed.

All things considered, unsupervised learning algorithms are valuable tools for detecting credit card fraud, helping businesses spot unusual activity and spot fraudulent cases in advance. Financial institutions can proactively fight against fraudulent activity and improve their fraud detection through threshold-based methods, forest splitting, aggregation methods and single-class classification methods in This will protect their customers and businesses from economic loss.

➢ *Ensemble Methods*

An important aspect of credit card fraud detection is ensemble techniques, which provide a sophisticated way to combine multiple machine learning techniques These techniques including boosting, bagging, random forests, stacking, and vote classifiers and the other methods are used to target fraud detection -To provide scheduling and to reduce overfitting variables Bagging methods—like random

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

forests—build decision trees trained on random subsets of data extensively and aggregate their predictions Bagging approaches Ensemble by transforming models and training data -improves stability and generalization performance.

AdaBoost and Gradient Boosting Machines (GBM) are two examples of algorithms that extend ensemble learning by iteratively improving models to focus on information misclassified by previous models. Through an iterative process of algorithm enhancement, handle well-classified models and they emphasize the robust, group composite - Performance can be further increased Furthermore, stacking is a sophisticated clustering process that leads to a meta-learner who learns to better balance the contributions of different models by making predictions from combining multiple base models by Through stacking, the cluster is better able to predict outcomes and was able to capture complex interactions in data by combining the strengths of different models.

In addition to these techniques, classifiers aggregate forecasts using a polling multiple or a weighted voting system, providing a simple but effective method for group learning Classifiers can draw strong conclusions even as individuals patterns are different. The ability to adapt is also important in credit-card fraud detection, where these group techniques play a key role. Ensemble techniques provide strong protection against fraudulent activities using mass intelligence of various patterns serve to safeguard financial transactions in the banking system and trust continues.[11]

- *Model Evaluation and Optimization*

Applying a multi-pronged approach to evaluating and optimizing models for credit card fraud detection to ensure that machine learning algorithms for detecting fraudulent activity are reliable and fly effectiveness is the first step in a comprehensive assessment appropriate to the unique needs and objectives of fraud detection systems.[6] The appropriate measures are selected. Of particular importance are precision, recall, and F1 scores because they shed light on the trade-off between correct detection of deceptive interactions and reduction of false alarms Moreover, precision provides a general view of the overall performance of the model, whereas the area under the customer operating characteristic (ROC) curve and the corresponding metric AUC, which is the range of a threshold.[11]

Cross-validation methods are important when assessing how well fraud detection models generalize. Cross-validation reduces the chances of overfitting smaller sets of data and increases flexibility by partitioning the dataset into several subsets and retraining and calibrating the model on these remaining subsets together with various surfaces, hyper parameter tweaking is necessary to increase the performance of the model. Two popular methods for analysing hyper parameter space and determining optimal parameters to improve model performance are network search and random search.

After being trained and refined by cross-validation and hyper parameter tuning, the model is validated on a different holdout set or test set. To evaluate model performance on untested data and ensure that it can generalize to real-world conditions, this validation phase is necessary to further improve model performance, ensemble techniques such as bagging, boosting, and stacking is used. Using individual observations, these ensemble methods enhance the robustness of fraud detection systems, reduce overfitting, and improve prediction accuracy. [7,8]

For long-term effectiveness and adaptation to changing fraud tactics, fraud detection systems must be continually monitored and upgraded. Organizations can develop robust and reliable fraud detection systems that use a variety of techniques to thoroughly review and optimize these systems to identify fraudulent transactions reducing false positives and fakes effectively manage adverse events to hedge financial transactions in the face of changing credit and banking conditions This holistic approach is essential to maintain confidence.

## V. FUTURE SCOPE

As technology advances and economic transactions shift to internet structures, the need for sophisticated credit card fraud detection system grows more vital than ever. Looking ahead, there are numerous viable possibilities for reinforcing these systems to keep up with more sophisticated fraudsters while also protecting purchasers and companies. Here, we examine a few feasible future prospects for credit card fraud detection systems and their ramifications.

- Enhanced Machine Learning Algorithms: While machine learning algorithms are widely employed in fraud detection systems, there's nonetheless capability for development. Future advances in machine learning strategies, along with deep learning and reinforcement techniques, could lead to more accurate and efficient fraud detection. These algorithms can better adapt to evolving fraud patterns and detect abnormalities in real time, reducing fake positives while boosting overall system performance.
- Big Data Analytics: As the number of digital transactions increase, the volume of data generated grows dramatically. Big data analytics approach can assist discover minor patterns and correlations that imply fraudulent activity. Credit card fraud detection systems instantly identify suspicious behaviour and take necessary measures by means of analysing huge amounts of transactional data in real time.
- Real-time monitoring and alerting: Timeliness is important for fraud detection and prevention. Future structures will most possibly focus on improving real-time monitoring abilities to discover fraudulent behavior as soon as it happens. Automated indicators can advise each customer and financial institutions of questionable activities, considering quick action to prevent fraudulent behavior and guard sensitive information.
- AI-powered chatbots: AI-powered chatbots with natural language processing (NLP) abilities can be extremely

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24APR939

beneficial in fraud detection and customer service. These chat questions indicated with users in actual time, confirming transactions, answering questions, and reporting questionable conduct. Financial institutions can use AI chatbots to perform proactive fraud detection while additionally imparting personalised and responsive customer service.

- Complex Authentication Methods: In addition to traditional passwords and PINs, future credit card fraud detection syatems may also use more complex authentication methods. These should contain biometric authentication (as an example, fingerprint or face recognition), two-factor authentication (2FA), or even blockchain-based identification verification. Implementing multi- factor authentication strategies will increase the boundaries to unauthorised access, decreasing the likelihood of a successful fraud attempts.

## VI. CONCLUSION

In conclusion, this research paper examined the essential significance of machine learning within the improvement of credit card fraud detection systems. A detailed assessment of the literature and analysis of numerous machine learning algorithms exhibits that machine learning procedures have excellent capability for detecting and blocking off fraudulent transactions in real time.

The paper emphasised the significance of characteristic engineering, model selection, and evaluation metrics in developing powerful fraud detection systems. Furthermore, the incorporation of current machine learning strategies including deep learning and ensemble approaches has confirmed promise in enhancing the accuracy and efficiency of fraud detection algorithms.

The report additionally emphasised the barriers and boundaries of credit card fraud detection, together with uneven datasets, converting fraud patterns, and computational complexity. Addressing these problems includes ongoing research at and the development of novel techniques to conform to changing fraud dynamics.

Overall, the information provided in these studies highlight the need of the usage of machine learning in combatting credit card fraud. Financial establishments may improve the safety of their customers' budget and hold consider in the digital price surroundings by of leveraging the power of data-driven techniques and constantly improving algorithms. As machine learning advances, it has significant capacity to enhance fraud detection systems and reduce the risks linked with monetary fraud.

## ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all those who have contributed to this project. Your support, guidance, and encouragement have been invaluable throughout this journey.” First and the foremost we, express our deep sense of gratitude, sincere thanks to Prof. Swati Shamkuwar for the best support, opinion, views, comments, and thoughts that have been extremely helpful.

## REFERENCES

[1]. Sailusha, R., Gnaneswar, V., Ramesh, R., and Rao, G.R., 2020, May. Credit card fraud detection using machine learning. In *2020 4th international conference on intelligent computing and control systems (ICICCS)* (pp. 1264-1270). IEEE.

[2]. Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., and Singh, A.K., 2021. Credit card fraud detection using machine learning: a study. *arXiv preprint arXiv:2108.10005*.

[3]. Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, *29*(5), pp.3414-3424.

[4]. Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M., 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, *10*, pp.39700-39715.

[5]. Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A. and Aljaaf, A.J., 2020. A systematic review on supervised and unsupervised machine learning algorithms for data science. *Supervised and unsupervised learning for data science*, pp.3-21.

[6]. Janiesch, C., Zschech, P. and Heinrich, K., 2021. Machine learning and deep learning. *Electronic Markets*, *31*(3), pp.685-695.

[7]. Lai, J.P., Chang, Y.M., Chen, C.H. and Pai, P.F., 2020. A survey of machine learning models in renewable energy predictions. *Applied Sciences*, *10*(17), p.5975.

[8]. Chatzimparmpas, A., Martins, R.M., Jusufi, I., Kucher, K., Rossi, F. and Kerren, A., 2020, June. The state of the art in enhancing trust in machine learning models with the use of visualizations. In *Computer Graphics Forum* (Vol. 39, No. 3, pp. 713-756).

[9]. Amr, T., 2020. *Hands-On Machine Learning with scikit-learn and Scientific Python Toolkits: A practical guide to implementing supervised and unsupervised machine learning algorithms in Python*. Packt Publishing Ltd.

[10]. Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), p.24.

[11]. Khatri, S., Arora, A., and Agrawal, A.P., 2020, January. Supervised machine learning algorithms for credit card fraud detection: a comparison. In *2020 10th international conference on cloud computing, data science & engineering (confluence)* (pp. 680-683). IEEE.