AMERICAN Journal of Public Diplomacy and International Studies
Volume 02, Issue 10, 2024 ISSN (E):2993-2157

Revolutionizing Credit Card Fraud Detection: Harnessing Machine Learning and Data Science for Enhanced Security

R. Regin
Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, India

S. Suman Rajest
Professor, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India

Abstract: Credit cards allow you to make purchases, debt transfers, and cash advances but require you to repay the loan. Credit cards have been important over the last few decades because they allow us to collect incentives without changing our spending habits. It also simplifies spending tracking. Credit cards protect against fraud better than debit and are safer than cash. Responsible credit card use is a fast and easy approach to improve credit. Diners Club was the first contemporary credit card, founded in 1950. Cheap products and services can be purchased using a credit card. However, credit card fraud is common due to lost or stolen credit cards, skimming your credit card at a gas station pump, hacking your computer, calling about fake prizes or wire transfers, phishing attempts, looking over your shoulder at checkout and stealing your mail, etc. With unsupervised machine learning methods, we will use unlabeled data in this project to find patterns and dependencies in the credit card fraud detection dataset, allowing us to group data samples by similarities without manual labelling and detect frauds.

Keywords: Detect And Prevent These Frauds; Unsupervised Machine Learning; Hacking Your Computer; Detection Dataset; Location Scanning; Stealing Your Mail.

Introduction

Over the last few decades, credit cards have become an integral part of financial transactions, providing a convenient and secure alternative to cash. With features such as fraud protection and ease of use, responsible credit card usage serves as one of the quickest methods to build credit. However, alongside these benefits lies the ever-growing threat of credit card fraud, a serious issue that impacts millions of consumers and businesses each year [6-11].

Credit card fraud occurs when an unauthorized individual gains access to a person's credit card information to make fraudulent purchases [12-19]. This can happen through various means, such as lost or stolen cards, skimming devices at gas stations or ATMs, hacking into computers, phishing scams via fake emails, and even simple acts like shoulder surfing at checkout lines. Additionally, physical theft of mail containing credit card information remains a significant risk [20-26]. The financial ramifications of credit card fraud are substantial, with billions of dollars lost annually. According to various studies, the cost of fraud extends beyond immediate monetary losses, affecting the trust between consumers and financial institutions, and leading to increased security measures that can burden both parties. As a result, efficient fraud detection systems are vital to safeguarding consumers and preventing further financial exploitation [27-31].

In recent years, advancements in machine learning (ML) and data science have transformed the landscape of fraud detection. Traditional methods of fraud detection often relied on manual rules and historical data analysis, which can be inadequate given the rapidly evolving nature of fraudulent activities [32-39]. Machine learning enables the automatic identification of patterns and anomalies within vast datasets, allowing for quicker and more accurate fraud detection. Unsupervised machine learning methods are particularly beneficial in credit card fraud detection. These techniques allow the identification of patterns and groupings in data without requiring prior labeling. For instance, clustering algorithms can categorize transaction data based on similarities, making it easier to spot unusual behaviors indicative of fraud [40-45]. By analyzing large volumes of transaction data, unsupervised learning can reveal hidden structures and trends, providing insights that may not be visible through traditional analysis.

Fraud detection involves analyzing various features related to user behavior, transaction history, and geographic location. User spending patterns can provide insights into what constitutes "normal" behavior for an individual, while deviations from these patterns may signal potential fraud. Similarly, geographic analysis can reveal inconsistencies, such as a transaction occurring in a location far from the user's usual spending area [46-52]. Machine learning models can be trained to recognize these behavioral patterns by processing historical transaction data. For instance, a model might learn that a user typically makes purchases in their home city and rarely spends over a certain threshold. If a transaction appears in a foreign country or exceeds their typical spending limit, the model may flag it for further investigation [53-61].

When developing a fraud detection system, selecting the right machine learning algorithm is crucial. Various classifiers have been proposed for this purpose, including logistic regression, decision trees, random forests, and neural networks. Each algorithm has its strengths and weaknesses, and the choice of classifier can significantly impact the system's performance [62-69]. The effectiveness of a machine learning model is often measured through metrics such as accuracy, precision, recall, and the F1 score. In the context of credit card fraud detection, high precision is particularly important, as it minimizes false positives—situations where legitimate transactions are incorrectly flagged as fraudulent. Meanwhile, high recall ensures that most fraudulent transactions are identified. Using techniques like cross-validation and grid search, practitioners can fine-tune their models and select the optimal parameters for better performance. Additionally, ensemble methods, which combine multiple algorithms, can further enhance accuracy and reliability [70-78].

The success of any machine learning initiative heavily depends on the quality and quantity of the data used for training. In the case of credit card fraud detection, a diverse and comprehensive dataset is crucial. This dataset should include a wide range of transaction types, user demographics, and historical fraud cases [79-85]. By incorporating a rich set of features, the machine learning model can develop a more nuanced understanding of what constitutes fraudulent behavior. Data preprocessing is another essential step in the machine learning pipeline. This involves cleaning the dataset by handling missing values, normalizing data, and encoding categorical variables. Ensuring data quality can greatly improve the model's ability to generalize and detect fraud accurately [86-92].

One of the compelling benefits of applying machine learning to credit card fraud detection is the ability to visualize fraud patterns. Data visualization techniques, such as 3D modeling, can be employed to represent complex relationships within the data [93-101]. This visual representation can help analysts identify clusters of fraudulent activity and understand how different features interact to influence fraud risk. For instance, visualizing transaction data by geographical location can reveal hotspots of fraudulent activity. By mapping these areas, financial institutions can allocate resources more effectively to monitor and respond to potential threats [102-109].

As technology continues to evolve, so too will the methods used for fraud detection. Emerging techniques such as deep learning offer exciting possibilities for further improving detection systems. Neural networks, particularly convolutional neural networks (CNNs), have shown

promise in identifying intricate patterns in large datasets [110-116]. Moreover, integrating real-time data processing and predictive analytics can enhance the speed and accuracy of fraud detection systems. By analyzing transaction data in real-time, financial institutions can respond to suspicious activities more swiftly, potentially preventing fraud before it occurs [117-121].

Credit card fraud detection is an essential area of focus for financial institutions aiming to protect consumers and mitigate financial losses. By leveraging the power of machine learning and data science, organizations can develop sophisticated models that analyze user behavior, identify fraudulent patterns, and improve overall security [122-129]. The application of unsupervised learning techniques, the careful selection of classifiers, and a commitment to data quality are critical components of successful fraud detection initiatives. As the landscape of fraud continues to evolve, ongoing research and development in machine learning will be pivotal in staying one step ahead of fraudulent activities, ultimately fostering a safer financial environment for consumers everywhere [130].

Methodology

A credit card fraud detection project utilizing machine learning and data science begins with clearly defining the problem statement and setting specific objectives. This foundational step guides the entire project. The next phase involves collecting transactional data from multiple sources, including banks, credit card companies, and merchants, to ensure a comprehensive dataset.

Once the data is collected, it undergoes pre-processing, which includes cleaning to remove any inaccuracies, transforming the data into a suitable format, and normalizing values to maintain consistency. Following this, feature selection is performed to identify the most relevant variables that will aid in training the machine learning models effectively.

After selecting the appropriate features, the project moves on to training various machine learning models using the pre-processed data. Algorithms such as decision trees, random forests, and neural networks can be employed to assess their performance in detecting fraudulent transactions [131-135]. Once the models are trained, they are evaluated using key metrics like accuracy, precision, recall, and F1 score. This evaluation process helps identify the best-performing model for the task.

The final step is deploying the optimized model into a production environment, where it can detect and prevent fraudulent transactions in real-time. Continuous monitoring and maintenance of the deployed model are crucial to ensure its effectiveness. As new data becomes available, the model should be updated and retrained to adapt to evolving fraud patterns, thereby enhancing its performance over time. This iterative process ensures that the system remains robust against emerging threats, ultimately protecting consumers and financial institutions from fraud.

2. Literature review

The paper authored by [1] explores the application of supervised classification techniques for credit card fraud detection using Bayesian network classifiers. Specifically, it examines classifiers such as K2, Tree Augmented Naive Bayes (TAN), Naive Bayes, logistic regression, and J48 decision trees. The focus on these classifiers allows for a comprehensive analysis of their effectiveness in identifying fraudulent transactions. One of the key advantages highlighted in the study is the significant improvement in accuracy achieved after pre-processing the dataset. By employing techniques like normalization and principal component analysis, all classifiers reached over 95% accuracy. This demonstrates the critical role that data preparation plays in enhancing model performance, underscoring the importance of effective preprocessing steps in machine learning workflows. However, the study also points out certain limitations and areas for future exploration. The authors express an intention to investigate credit card fraud detection using real-time data, which could provide a more dynamic understanding of fraudulent behaviors. Additionally, since the Bayesian network classifiers yielded superior results, future research may benefit from comparing them with other types of classifiers, such as hyperplane-

based classifiers. This comparison could further enrich the body of knowledge in the field and potentially lead to the development of even more effective fraud detection methodologies.

The paper authored by [2] offers a thorough review of various machine learning techniques employed in credit card fraud detection. It discusses methods such as decision trees, support vector machines, and neural networks, highlighting their applications and effectiveness in identifying fraudulent transactions. This comprehensive overview serves as a valuable resource for both researchers and practitioners in the field, enabling them to understand the landscape of current techniques and their respective functionalities. However, the paper does have limitations. Notably, it lacks a comparative analysis of the discussed techniques, which makes it challenging for readers to determine which method may be the most effective for specific contexts or datasets. Without such a comparison, stakeholders may struggle to make informed decisions regarding the selection of appropriate algorithms for their fraud detection systems. Future research could enhance the discourse by including direct performance evaluations, thus providing clearer insights into the advantages and drawbacks of each machine learning approach. This would ultimately contribute to a more nuanced understanding of how to combat credit card fraud effectively.

The paper by [3] presents an extensive survey of various machine learning algorithms used for credit card fraud detection. The authors delve into a range of techniques, including random forest, support vector machines, artificial neural networks, naive Bayes, logistic regression, and decision trees. This comprehensive overview not only highlights the capabilities of each algorithm but also addresses the challenges and limitations associated with these methods. By discussing these aspects, the authors provide valuable insights that can guide future research in the field of fraud detection. However, a notable limitation of the paper is the absence of a comparative analysis among the algorithms. Without such a comparison, it becomes challenging for readers to ascertain which algorithm might be the most effective for credit card fraud detection in various scenarios. The lack of direct performance evaluations means that stakeholders may find it difficult to make informed decisions when selecting an appropriate method for their specific needs. Future studies could enhance the understanding of these algorithms by including comparative metrics, thereby aiding practitioners in choosing the best-suited approach for their fraud detection systems.

The paper authored by [4] focuses on a hybrid machine learning approach to credit card fraud detection. It employs a combination of classifiers, specifically artificial neural networks, decision trees, and k-nearest neighbors, to enhance detection accuracy. The authors demonstrate that their proposed hybrid algorithm significantly outperforms traditional machine learning methods, particularly in the context of imbalanced datasets, which are prevalent in fraud detection scenarios. This advancement is noteworthy as it addresses a common challenge in the field, improving the reliability of fraud detection systems. However, the study has certain limitations. One notable drawback is the exclusion of deep learning algorithms, which have shown promising results in various recent studies. Deep learning techniques, known for their ability to handle complex patterns and large datasets, could potentially offer further improvements in fraud detection accuracy. By not considering these advanced methods, the paper may overlook opportunities to enhance its proposed algorithm. Future research could explore the integration of deep learning approaches with the hybrid model, potentially leading to even more robust solutions for credit card fraud detection.

In their paper [5] present a novel approach to credit card fraud detection using convolutional neural network autoencoders. This deep-learning framework leverages advanced neural network architectures to enhance the detection process, significantly outperforming traditional machine learning algorithms. The authors demonstrate that their method achieves high accuracy rates while maintaining low false positive rates, making it a promising solution for identifying fraudulent transactions. However, a notable limitation of the study is its reliance on synthetic datasets for evaluation. The absence of real-world data makes it challenging to assess the practicality and robustness of the proposed approach in actual financial environments. This gap

highlights the need for further research that tests the model under more realistic conditions to validate its effectiveness in combating credit card fraud.

Project description

By addressing the shortcomings of earlier systems, the suggested system improves the security of the user's private data. Businesses would be safeguarded from heavy losses under the proposed approach, which relies on automated machine learning systems to make smart decisions. There is much less danger while doing business online thanks to these precautions. Machine learning algorithms, similar to people, can learn from transaction data in the past and apply that knowledge to future transactions. The benefit of using machines comes in the speed of data processing and computing, even though they may not be as intelligent as humans and may require additional supervision. In addition, when faced with massive amounts of data, machines are better able to spot patterns and retain them than people are. These algorithms are often referred to as anomaly detectors. What follows is an in-depth discussion of the topic.

Module description

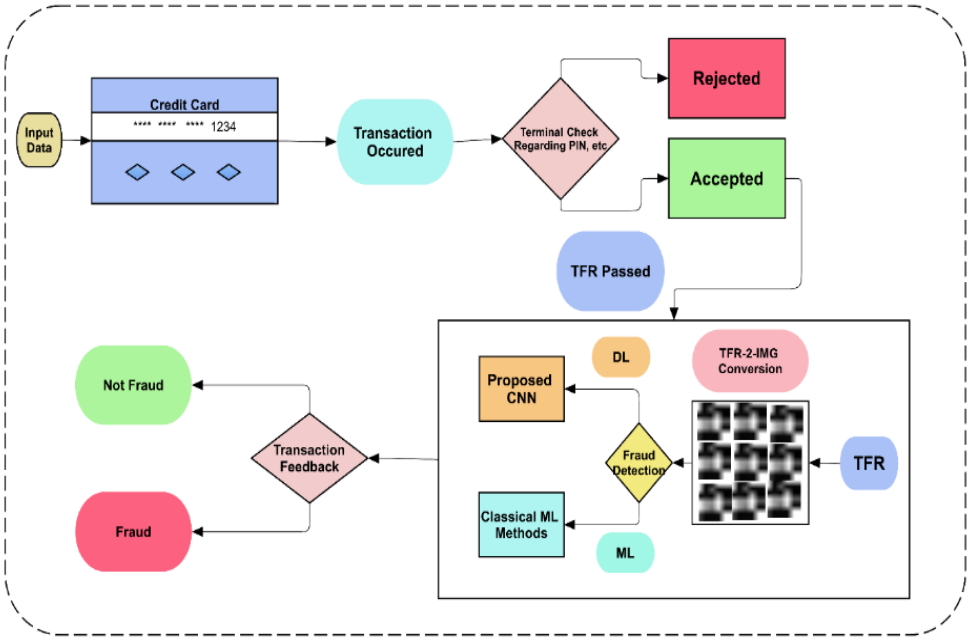

Figure 1. Credit card fraud detection architecture diagram

Figure 1 represents the credit card fraud detection architecture diagram of the project. The input data is first given to the credit card, which, on authorization transcends to the process of any transaction needing to take place. After the transaction request is authorised, it further goes through a process of terminal check regarding the pin, asking for it. On the pin being correct or wrong, access to money in the account is accepted or rejected respectively. If the terminal check allows further access, then a trf is passed, where the trf images are converted for fraud detection. If the dl is a proposed CNN or the ml is a classical ml method, then based on the transaction feedback from the data collected gives us a result of whether the transaction process was an attempt at fraud or not. The customer first sends a login request to the machine, and whether the login details of the account are valid is provided with access or not. The user information entered is cross-checked with the available customer database, and the account details are verified to grant access. If the information entered is not valid, then a fraud alert database is activated, checked, and then reported to the agent, saying it is a "fraud alert message." If it is a valid user, they are asked to verify card details monitored by an agent and then given access to their account.

Module description

One possible placement for the pre-processing segment is just before the data coaching and testing phases. One of the most popular fraud detection tools in the technical industry is AVS. The input data is subjected to a variety of procedures throughout the test data pre-processing step in order to detect a multitude of fraud tendencies. Due to the presence of undesired information and sounds, the raw card transactions obtained from the bank and other sources are not suitable for direct processing. Consequently, pre-processing the input data is necessary prior to analysis. All digital applications require input dataset pre-processing before processing operations such as pattern classification and segmentation can begin (Figure 2).

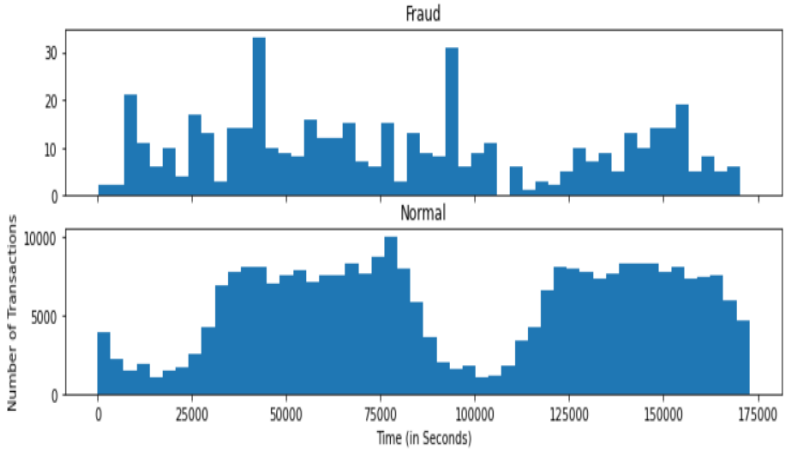

Figure 2: Pre-Processing of Data

By identifying areas that share characteristics like colour, texture, contrast, and grey level, segmentation can divide an image into more manageable pieces. Objects in an image can be divided up using segmentation. The goal of fraud pattern segmentation is to find hotspots—places with a high fraud rate or areas where frauds happen frequently—by studying the systematic structure of fraud patterns. So far, we have categorised segmentation methods according to grey-level-based and textural feature-based approaches, both of which are applicable to the processing of fraud patterns. The data is then divided into two sets, training data and testing data, with the former making up 70% and the latter 30% respectively after the pre-processing phase. A area of interest (ROI) can be extracted for the purpose of transaction analysis through feature extraction. Transforming the dataset from one level of transactions to another is part of it. It is possible to glean valuable insights from these more complex interactions. The primary objective of this study is to identify the most effective feature extraction approach for the purpose of valid transaction classification. In this study, the most popular approaches for extracting features from medical pictures are support vector machines (SVMs), clustering techniques, k-nearest neighbour algorithms, neural networks, naive Bayes classifiers, and Adaboost and majority voting (amv).

Testing the model involves a series of processes to ensure it can make accurate predictions. Using the testing set to make predictions is the initial stage. Training and testing are the two main components of classification, a supervised learning process. A training set is used to teach the classifier new skills during the training phase. When a classifier is in testing, it is put to the test on samples it is unfamiliar with. To back up smart decisions, knowledge-based systems use AI technologies that operate in a confined domain. Acquiring and representing knowledge makes use of a wide range of knowledge representation strategies, frameworks, scripts, and rules. Information documentation, intelligent decision assistance, self-learning, reasoning, and explanation are the fundamental benefits of this kind of technology.

Finding patterns of credit card fraud is possible with the help of a number of instruments. Recently, there has been an uptick in credit card fraud. The majority of fraud incidents take place over the internet. If you have your credit card information on file, a fraudster may attempt to break into your system and use it. Similar to the similarity tree, this decision tree uses the same rationale. Attributes and factors are contained inside its leaves and nodes. In order to meet certain requirements, this method is useful for defining ratios in relation to transactions. In order to detect behavioural fraud, tools including clustering techniques, predictive analytics, and algorithms are utilised. Credit card fraud detection using peer group analysis is a well-liked clustering technique. It finds instances where a credit card account is acting suspiciously in relation to other accounts. In order to train and accomplish particular patterns, fraud detection methods such as K-nearest neighbour algorithms, neural networks, and supervised, unsupervised, reinforcement learning, and other machine learning algorithms are applied to an input dataset.

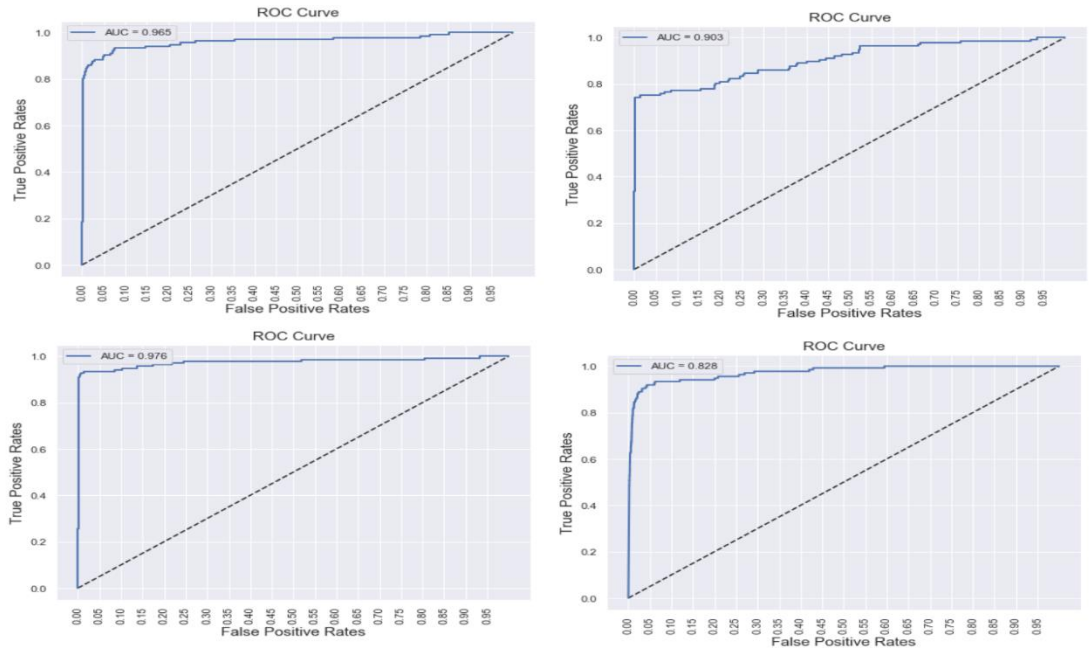

Figure 3: Input graph of the trained dataset

Figure 3 displays the results, which demonstrate trends in the creation and use of a machine learning model for the detection of credit card fraud. The training process for the machine learning algorithm involves analysing a dataset with a collection of transactions. The goal is to determine which data properties, when applied, will lead to the trained output graph accurately classifying the transactions as fraudulent or not, according to the model in the trained dataset.

Results and discussions

Here, we present a credit card fraud detection system that, with the aid of a collection of input datasets and machine learning algorithms, can determine which characteristics of a fraud pattern, when applied, will lead to the accurate categorization of a fraud event. The optimal combination to detect and prevent these scams is then determined by the machine learning algorithm system. There are a variety of approaches, and they all have their advantages and disadvantages. The majority of these machine learning techniques have open-source counterparts, which makes them accessible for experimentation with datasets.

When it comes to detecting fraud patterns, machine learning algorithms work wonders. Supervised and unsupervised ML segmentation and classification approaches were defined in this research. In order to train their mathematical models, supervised learning algorithms first need a collection of labelled data, in this case transactions. The following methods are examples of supervised machine learning: k-nearest neighbours (k-nn), support vector machines (SVM), decision trees (DT), linear regression, logistic regression, random forest (rf), artificial neural networks (ANN), gradient boosting, and naïve Bayes models. In unsupervised learning, the

output labels are not necessary for the mathematical models that are created. Algorithms sort data according to patterns they find. Principal component analysis (PCA), fuzzy c-means, apriori algorithm, k-means clustering, hierarchical clustering, and other similar unsupervised machine learning techniques (FCM).

Among the many components of the current system are algorithms designed to detect fraudulent behaviour; for example, credit card companies employ complex algorithms to examine patterns of transactions in order to spot suspicious behaviour. If a customer's spending habits suddenly changed or showed other signs of suspect activity, these algorithms would alert the system. Additional approaches include things like better authentication, customer notifications, human review, chargeback monitoring, and so on. These strategies were effective up to a point, but modern card frauds use sophisticated patterns that our current systems are ill-equipped to detect. The suggested solution also use machine learning algorithms to spot fraudulent or otherwise suspicious credit card purchases. Anomaly detection, continuous learning, real-time decision-making, predictive modelling, and other machine learning algorithmic approaches are utilised.

Conclusion

Due to the simplification of authentication procedures brought about by advances in electronic financial transaction technology and the rise of simple payment, the possibility of fraudulent payment and fraudulent payment has increased. There are several forms of credit card fraud, including but not limited to: theft and loss, identity theft, card forgery, new card not received, and card information theft. Phishing, pharming, and the accidental disclosure or theft of credit card information are among the most common forms of online fraud. In an effort to combat this growing problem, the government launched the "e-financial fraud prevention service." Simply configuring the current keyboard security, public certificate, and extra password is not enough to deal with financial fraud. Financial institutions and users are kept informed by the anomalous transaction detection system, which analyses user and payment data in real-time. If the data is different from the usual pattern, the system arbitrarily stops the transaction and notifies both parties. Hence, for quick and reliable identification, an anomalous transaction detection system is crucial, and further study is required to refine the algorithm. This research looked into the possibility of identifying suspicious transactions by analysing electronic payment logs and applying a machine learning algorithm. Efficient classification is carried out, and results demonstrate the relevance of techniques applied to the dataset. Using someone else's credit card without their permission is definitely dishonest. In this project, we compiled a list of the most popular fraud detection technologies and analysed the most current research in this area. The project has provided a thorough explanation of how machine learning can be used to improve fraud detection. It has included the method, pseudocode, implementation details, and experimental data. When only a tenth of the dataset is considered, the algorithm's accuracy drops to 28 percent, even though it reaches over 99.6 percent. On the other hand, when the algorithm is fed the heathenise dataset, the accuracy increases to 33%. Given the large discrepancy between the amount of legitimate and authentic transactions, it is not surprising that this % of accuracy is so high.

Future enhancements

Despite the impressive results achieved by hybrid approaches to fraud pattern identification utilising machine learning, there are still certain limits to consider. Machine learning used to be more dependent on structured input, and many methods might fail to train with even a single missing data point. There has been a renaissance in machine learning thanks to the new algorithms and the dramatic improvements in computing power and data availability. The series of actions taken to develop the model that will be used to predict classes from the features of the training samples most accurately. The "real-world" testing sometimes makes use of a third group of examples. In its iterative pursuit of optimal performance on the validation set, the algorithm system might pick up on specific traits from the training set. If the algorithm does well on a "unseen" test set, it raises the likelihood that it will produce accurate results when applied in the

actual world. Credit card fraud detection using machine learning algorithms has come a long way, but there are still a lot of loopholes that need fixing. In the selected domain, much remains unfinished business.

References

1. C. Phua and v. Lee, Kate smith1&rossgayler2 "A comprehensive survey of data mining-based fraud detection research" published by School of Businesses, Faculty of Information Technology Wellington Road, Clayton, Victoria; Australia, vol.12, no.2, pp.1243-1257,2020
2. C. Liu, Y. Chan, S. H. Alam kazmi, and h. Fu, "Financial fraud detection model: based on random forest," int. j. econ. Finance, vol.7, no.7, pp.178-188,2015.
3. J. Chawla, A. K. Ahlawat, “A Proposed Architecture for Local Host and Amazon Web Service with Multi-Agent System,” Intelligent Automation & Soft Computing, vol. 36, no. 3, pp. 2787–2802, March 2023.
4. J. Chawla, A. K. Ahlawat, “Resolving Software Interoperability Issues of Unsigned Number and Date-Time Precision Using JADE Framework System,” International Journal of System of Systems Engineering, Inderscience, vol. 11, no. 3/4, pp. 380-398, March 2022.
5. J. Chawla, A. K. Ahlawat, “Resolving Interoperability Issues of Date with Null Value and Collection of Complex Data Types by Using JADE-WSIG Framework,” Webology, vol. 18, no. 1, April 2021.
6. J. Chawla, A. K. Ahlawat, and J. Gautam, “Resolving Interoperability Issues of Precision and Array with Null Value of Web Services Using WSIG-JADE Framework,” Modelling and Simulation in Engineering, October 2020.
7. P. Bhardwaj, V. Bali, J. Kaur, “A Review on Load Balancing and Site Selection of Electric Vehicle Charging Station,” Test Engineering & Management, pp. 12437-12448, May-June 2020.
8. P. Bhardwaj, V. Bali, J. Kaur, “Improving the Efficiency of Load Balancing and Site Selection of Electric Vehicle Charging Station Using Dijkstra Algorithm,” Journal of Critical Reviews, vol. 7, no. 19, August 2020.
9. S. Banala, “The Future of IT Operations: Harnessing Cloud Automation for Enhanced Efficiency and The Role of Generative AI Operational Excellence,” International Journal of Machine Learning and Artificial Intelligence, vol. 5, no. 5, pp. 1–15, Jul. 2024.
10. S. Banala, "DevOps Essentials: Key Practices for Continuous Integration and Continuous Delivery," International Numeric Journal of Machine Learning and Robots, vol. 8, no. 8, pp. 1-14, 2024.
11. M. R. M. Reethu, L. N. R. Mudunuri, and S. Banala, “Exploring the Big Five Personality Traits of Employees in Corporates,” FMDB Transactions on Sustainable Management Letters, vol. 2, no. 1, pp. 1–13, 2024.
12. S. Banala, “The Future of Site Reliability: Integrating Generative AI into SRE Practices,” FMDB Transactions on Sustainable Computer Letters, vol. 2, no. 1, pp. 14–25, 2024.
13. B. Senapati and B. S. Rawal, "Adopting a deep learning split-protocol based predictive maintenance management system for industrial manufacturing operations," in Big Data Intelligence and Computing. DataCom 2022, C. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds., Lecture Notes in Computer Science, vol. 13864. Singapore: Springer, 2023, pp. 25–38.

14. B. Senapati and B. S. Rawal, "Quantum communication with RLP quantum resistant cryptography in industrial manufacturing," Cyber Security and Applications, vol. 1, 2023, Art. no. 100019.

15. B. Senapati et al., "Wrist crack classification using deep learning and X-ray imaging," in Proceedings of the Second International Conference on Advances in Computing Research (ACR'24), K. Daimi and A. Al Sadoon, Eds., Lecture Notes in Networks and Systems, vol. 956. Cham: Springer, 2024, pp. 72–85.

16. B. Kumar, M. H. S. Al Hasani, "Database Security—Risks and Control Methods," in 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), 2016, pp. 334-340.

17. B. Kumar and S. R. Alraisi, "Deepfakes Audio Detection Techniques Using Deep Convolutional Neural Network," in 2022 International Conference on Machine Learning Big Data Cloud and Parallel Computing (COM-IT-CON), vol. 1, pp. 463-468, 2022.

18. B. Kumar and H. Shaker, "Design and Execution of Secure Smart Home Environments on Visual Simulation Tool," in 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), pp. 262-280, 2023.

19. B. Kumar and O. Al Falhi, "Digital Transformation Through APIs," in 2022 International Conference on Machine Learning Big Data Cloud and Parallel Computing (COM-IT-CON), vol. 1, pp. 623-628, 2022.

20. B. Kumar, H. Shaker, B. Al Ruzaiqi, and R. Al Balushi, "Design and Implementation of a Smart Office Network Module Using Visual Simulation Tool," Journal of Namibian Studies: History Politics Culture, vol. 34, pp. 2664-2676, 2023.

21. K. Al-Aufi and B. Kumar, "Security Testing of Android Applications Using Drozer," in International Conference on Computational Sciences and Sustainable Technologies, Springer, 2023, pp. 89-103.

22. D. Dayana, T. S. Shanthi, G. Wali, P. V. Pramila, T. Sumitha, and M. Sudhakar, "Enhancing usability and control in artificial intelligence of things environments (AIoT) through semantic web control models," in Semantic Web Technologies and Applications in Artificial Intelligence of Things, F. Ortiz-Rodriguez, A. Leyva-Mederos, S. Tiwari, A. Hernandez-Quintana, and J. Martinez-Rodriguez, Eds., IGI Global, USA, 2024, pp. 186–206.

23. J. Tanwar, H. Sabrol, G. Wali, C. Bulla, R. K. Meenakshi, P. S. Tabeck, and B. Surjeet, "Integrating blockchain and deep learning for enhanced supply chain management in healthcare: A novel approach for Alzheimer's and Parkinson's disease prevention and control," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 22s, pp. 524–539, 2024.

24. R. K. Meenakshi, R. S., G. Wali, C. Bulla, J. Tanwar, M. Rao, and B. Surjeet, "AI integrated approach for enhancing linguistic natural language processing (NLP) models for multilingual sentiment analysis," Philological Investigations, vol. 23, no. 1, pp. 233–247, 2024.

25. G. Wali and C. Bulla, "Suspicious activity detection model in bank transactions using deep learning with fog computing infrastructure," in Advances in Computer Science Research, 2024, pp. 292–302.

26. G. Wali, P. Sivathapandi, C. Bulla, and P. B. M. Ramakrishna, "Fog computing: Basics, key technologies, open issues, and future research directions," African Journal of Biomedical Research, vol. 27, no. 9, pp. 748–770, 2024.

27. B. Kumar, I. Albusaidi, and M. Halloush, "Healthcare Information Exchange Using Blockchain and Machine Learning," in 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), pp. 55-69, 2023.

28. B. Al Barwani, E. Al Maani, and B. Kumar, "IoT-Enabled Smart Cities: A Review of Security Frameworks Privacy Risks and Key Technologies," in 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), pp. 83-95, 2023.

29. A. Hamza and B. Kumar, "A Review Paper on DES AES RSA Encryption Standards," in 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), pp. 333-338, 2020.

30. S. Al Busafi and B. Kumar, "Review and Analysis of Cryptography Techniques," in 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), pp. 323-327, 2020.

31. M. Al Saadi and B. Kumar, "A Review on Elliptic Curve Cryptography," Int. J. Future Gener. Commun. Netw., vol. 13, pp. 1597-1601, 2020.

32. TP. Krishna Kumar, M. Ramachandran, Kurinjimalar Ramu and Ashwini Murugan. "Analysis of Reverse Logistics System using COPRAS MCDM Method", REST Journal on Banking, Accounting and Business, Vol.1, no.4, pp.31, 2022.

33. TP. Krishna Kumar, M.Ramachandran, Chinnasami Sivaji and Chandrasakar Raja. "Financing practices of Micro and Small Entrepreneurs using WSM MCDM Method" , REST Journal on Data Analytics and Artificial Intelligence, Vol.1,no.4, pp.18, 2022

34. TP. Krishna Kumar TP, M. Ramachandran,Vidhya Prasanth, Chandrasekar Raja. "Developing Business Services Using IBM SPSS Statistics", REST Journal on Banking, Accounting and Business, Vol.2, no.1, pp. 40, 2023.

35. TP. Krishna Kumar, M. Ramachandran, Kurinjimalar Ramu, Ashwini Murugan. "Using this DEMATEL Corporate social responsibility CSR", REST Journal on Banking, Accounting and Business, Vol.2,no.1, pp.51. 2023.

36. Muhamed Rafi, Jabir Moosa, TP.Krishna Kumar, K.Deepak. "Crude Oil Price Influence on the Performance of Selected Stocks from Different Sectors – An Empirical Analysis", Journal of Survey in Fisheries Science, Vol.10, no.special 3, pp. 1893, 2023.

37. SK.Saravanan, R. Krishnamoorthy, TP. Krishna Kumar, R. Narayana rao, D. Udaya suriya Rajkumar, R. Thiagarajan, (2023). "IoT Alert Reflexion of Forbidden Deforestation Regions with Drone observation", The IEEE Xplore, Vol.18,no.5, pp.201. 2023

38. TP. Krishna Kumar, Purnendu Bikash Acharjee, Pravin Dnyaneshwar Sawant, Poonam Dabaria, A. Sulthan Mohideen, "The Impact of Using Facebook on Consumer Buying Behaviour in Online", Journal of Chemical Health Risks, Vol.12, no.s. 4, pp.744, 2023.

39. TP. Krishna Kumar, Priyanka Malhotra, B. Madhukumar, M.Maria Antony Raj, R.Augustian Isaac, D. Balasubramanian, "Exploring The Factors Influencing The Effectiveness Of Digital Marketing In Changing Environment; A Theoretical And Empirical Investigation", Journal of Educational Administration: Theory and Practice, Vol.30, no.4, pp.7488, 2024.

40. TP.Krishna Kumar, R. Suriakala, N. Shankar, M. Deepak, "Global To Local Perspectives In Succession Planning Of Family Business In Unorganized Sector", Journal of Educational Administration: Theory and Practice, Vol.30, no.5, pp.3056. 2024.

41. Ramírez, N. J. G., Polo, O. C. C., Gaviria, D. A. G., Ochoa, J. A. V., Arango, D. A. G., & Vásquez, J. A. U. (2024). El perfil del Contador Público, ¿una respuesta a las necesidades

organizacionales de las entidades sin fines de lucro en la Cuarta Revolución Industrial?. Revista de Gestão Social e Ambiental, 18(6), e05752-e05752.

42. Ramírez, Nini Johanna Guisao, et al. "El perfil del contador público, ¿una respuesta a las necesidades organizacionales de las entidades sin fines de lucro en la Cuarta Revolución Industrial?". Revista de Gestão Social e Ambiental 18.6 (2024): e05752-e05752.
43. Polo, O. C. C., Gaviria, D. A. G., Ochoa, J. A. V., Acosta, J. C. C., & Ruiz, J. A. M. (2024). Medellín District of Science, Technology and Innovation: An Opportunity to Reinforce the Curriculum of the Public Accounting Program with Artificial Intelligence?. Kurdish Studies, 12(2), 2791-2801.
44. Polo, Orlando Carmelo Castellanos, et al. "Medellín District of Science, Technology and Innovation: An Opportunity to Reinforce the Curriculum of the Public Accounting Program with Artificial Intelligence?." Kurdish Studies 12.2 (2024): 2791-2801.
45. Salazar, M. J. N., Henao, J. O. A., Uribe, H. A. N., Ochoa, J. A. V., Polo, O. C. C., & Ruiz, J. A. M. (2023). El impacto del impuesto sobre la renta en las finanzas personales en Colombia y Perú, 2019. Revista De Gestão E Secretariado, 14(11), 19533–19553.
46. M. J. N. Salazar, J. O. A. Henao, H. A. N. Uribe, J. A. V. Ochoa, O. C. C. Polo, e J. A. M. Ruiz, "El impacto del impuesto sobre la renta en las finanzas personales en Colombia y Perú, 2019", R. G. Secr., vol. 14, nº 11, p. 19533–19553, nov. 2023.
47. Orlando Carmelo Castellanos Polo, José Alexander Velásquez Ochoa, Paola Andrea Díaz Garcés, & Eudis Eugenia López Gómez. (2023). The Organizational Climate: How do public accounting students face the business dinosaur?. RES MILITARIS, 13(3), 894–903.
48. Orlando Carmelo Castellanos Polo, José Alexander Velásquez Ochoa, Paola Andrea Díaz Garcés, and Eudis Eugenia López Gómez, "The Organizational Climate: How do public accounting students face the business dinosaur?", RES MIL, vol. 13, no. 3, pp. 894–903, Mar. 2023.
49. Orlando Carmelo Castellanos Polo, Sandra Yaneth Cañas Vallejo, Jose Alexander Velasquez Ochoa, & Yesid González-Marín. (2023). The fiscal competition of the states from an international context. Res Militaris, 13(2), 3504–3509.
50. Orlando Carmelo Castellanos Polo, Sandra Yaneth Cañas Vallejo, Jose Alexander Velasquez Ochoa, and Yesid González-Marín, "The fiscal competition of the states from an international context", RES MIL, vol. 13, no. 2, pp. 3504–3509, Feb. 2023
51. Polo, O. C. C., Ochoa, J. A. V., & Acosta, J. C. C. (2023). Financial Statements in Accordance with IFRS 16 for Leases in the Context of COVID 19. International Journal, 10(1), 910-917.
52. Polo, Orlando Carmelo Castellanos; OCHOA, Jose Alexander Velasquez; ACOSTA, Juan Carlos Cardona. Financial Statements in Accordance with IFRS 16 for Leases in the Context of COVID 19. International Journal, 2023, vol. 10, no 1, p. 910-917.
53. Polo, O. C. C., Ochoa, J. A. V., Zapata, J. A. S., & Arango, D. A. G. (2023). Estado de la cuestión sobre tributación internacional. Revisión sistemática desde las directrices de prisma. Administración & Desarrollo, 53(1), 1-16.
54. Polo, Orlando Carmelo Castellanos, et al. "Estado de la cuestión sobre tributación internacional. Revisión sistemática desde las directrices de prisma." Administración & Desarrollo 53.1 (2023): 1-16.
55. Ochoa, J. A. V., Polo, O. C. C., Acosta, J. C. C., & Arboleda, W. A. R. (2023). Cryptocurrencies: Legal Treatment In Various Jurisdictions. Russian Law Journal, 11(2), 54-58.

56. Ochoa, Jose Alexander Velasquez, et al. "Cryptocurrencies: Legal Treatment In Various Jurisdictions." Russian Law Journal 11.2 (2023): 54-58.

57. Polo, O. C. C., Ochoa, J. A. V., Sanmartin, A. F. S., & Arango, D. A. G. (2023). Tax Evasion, Corruption And Tax Administrative Management. Russian Law Journal, 11(2), 44-53.

58. Polo, Orlando Carmelo Castellanos, et al. "Tax Evasion, Corruption And Tax Administrative Management." Russian Law Journal 11.2 (2023): 44-53.

59. Polo, O. C. C., Ochoa, J. A. V., Posada, G. I. A., & Arcila, J. O. S. (2022). La auditoría forense¿ Un instrumento esencial de control interno en las entidades públicas?. Administración & Desarrollo, 52(1), 95-112.

60. Polo, Orlando Carmelo Castellanos, et al. "La auditoría forense¿ Un instrumento esencial de control interno en las entidades públicas?." Administración & Desarrollo 52.1 (2022): 95-112.

61. Polo, O. C. C., Ochoa, J. A. V., & Posada, G. I. A. (2021). La doble tributación internacional sobre la inversión directa extranjera en América Latina y el Caribe. Administración & Desarrollo, 51(1), 165-183.

62. Polo, Orlando Carmelo Castellanos, José Alexander Velásquez Ochoa, and Gladys Irene Arboleda Posada. "La doble tributación internacional sobre la inversión directa extranjera en América Latina y el Caribe." Administración & Desarrollo 51.1 (2021): 165-183.

63. Kumar, J., & Rani, V., "Investigating the dynamics of FinTech adoption: an empirical study from the perspective of mobile banking", Journal of Economic and Administrative Sciences, April 2024.

64. Kumar, J., Rani, G., Rani, M., & Rani, V, "Do green banking practices improve the sustainability performance of banking institutions? The mediating role of green finance", Social Responsibility Journal, July 2024.

65. Kumar, J., Rani, M., Rani, G., & Rani, V, "Human-machine dialogues unveiled: an in-depth exploration of individual attitudes and adoption patterns toward AI-powered ChatGPT systems", Digital Policy, Regulation and Governance, 26(4), 435-449, April 2024.

66. Kumar, J., Rani, V., Rani, G., & Rani, M. (2024). Understanding purchase behaviour towards green housing among millennials: the mediating role of purchase intention. International Journal of Housing Markets and Analysis, April 2024.

67. Kumar, J., & Rani, V. (2024). Financial innovation and gender dynamics: a comparative study of male and female FinTech adoption in emerging economies. International Journal of Accounting & Information Management, August 2024.

68. Kumar, J., Rani, G., Rani, M. and Rani, V. (2024). Blockchain technology adoption and its impact on SME performance: insights for entrepreneurs and policymakers. Journal of Enterprising Communities: People and Places in the Global Economy, Vol. ahead-of-print No. ahead-of-print, August 2024.

69. Kumar, J., & Rani, V., "What do we know about cryptocurrency investment? An empirical study of its adoption among Indian retail investors," The Bottom Line, February 2024, Vol. 37 No. 1, pp. 27-44.

70. Rani, V., & Kumar, J., "Gender differences in FinTech adoption: What do we know, and what do we need to know?", Journal of Modelling in Management.

71. Kumar, J., Rani, V., Rani, G., & Rani, M., "Does individuals' age matter? A comparative study of generation X and generation Y on green housing purchase intention," Property Management.

72. Kumar, J., Rani, M., Rani, G., & Rani, V., “What do individuals know, feel and do from a financial perspective? An empirical study on financial satisfaction”. International Journal of Social Economics. November 2023.

73. M. M. Islam and L. Liu, “Deep learning accelerated topology optimization with inherent control of image quality,” Structural and Multidisciplinary Optimization, vol. 65, no. 11, Nov. 2022.

74. S. Park et al., “Universal Carbonizable Filaments for 3D Printing,” Advanced Functional Materials, Jun. 2024.

75. M. M. Islam and L. Liu, “Topology optimization of fiber-reinforced structures with discrete fiber orientations for additive manufacturing,” Computers & Structures, vol. 301, pp. 107468–107468, Sep. 2024.

76. J. Cao, G. Bhuvaneswari, T. Arumugam, and A. B. R, "The digital edge: Examining the relationship between digital competency and language learning outcomes," Frontiers in Psychology, vol. 14, Jun. 2023.

77. J. Rehman, M. Kashif, and T. Arumugam, "From the land of Gama: Event attachment scale (EAS) development exploring fans’ attachment and their intentions to spectate at traditional gaming events," International Journal of Event and Festival Management, vol. 14, no. 3, pp. 363–379, Jun. 2023.

78. K. U. Kiran and T. Arumugam, "Role of programmatic advertising on effective digital promotion strategy: A conceptual framework," Journal of Physics: Conference Series, vol. 1716, p. 012032, Dec. 2020.

79. M. A. Sanjeev, A. Thangaraja, and P. K. S. Kumar, "Multidimensional scale of perceived social support: Validity and reliability in the Indian context," International Journal of Management Practice, vol. 14, no. 4, p. 472, 2021.

80. M. A. Sanjeev, S. Khademizadeh, T. Arumugam, and D. K. Tripathi, "Generation Z and intention to use the digital library: Does personality matter?," The Electronic Library, vol. 40, no. 1/2, pp. 18–37, Dec. 2021.

81. S. Gupta, N. Pande, T. Arumugam, and M. A. Sanjeev, "Reputational impact of COVID-19 pandemic management on World Health Organization among Indian public health professionals," Journal of Public Affairs, Oct. 2022.

82. S. Hameed, S. Madhavan, and T. Arumugam, "Is consumer behaviour varying towards low and high involvement products even sports celebrity endorsed?," International Journal of Scientific & Technology Research, vol. 9, no. 3, Mar. 2020. [Online]. Available: https://www.ijstr.org/final-print/mar2020/Is-Consumer-Behaviour-Varying-Towards-Low-And-High-Involvement-Products-Even-Sports-Celebrity-Endorsed.pdf

83. S. Verma, N. Garg, and T. Arumugam, "Being ethically resilient during COVID-19: A cross-sectional study of Indian supply chain companies," The International Journal of Logistics Management, Aug. 2022.

84. T. Arumugam, B. L. Lavanya, V. Karthik, K. Velusamy, U. K. Kommuri, and D. Panneerselvam, "Portraying women in advertisements: An analogy between past and present," The American Journal of Economics and Sociology, vol. 81, no. 1, pp. 207–223, Jan. 2022.

85. T. Arumugam, B. Subramaniam, B. Jayakrishnan, V. Asi, M. Reddy, and Ranganathan, "Financial reengineering perspectives of Government of India with respect to time series effect and performance of sovereign gold bond," Accessed: Aug. 06, 2024. [Online]. Available:https://www.ijstr.org/final-print/mar2020/Financial-Reengineering-Perspectives-Of-Government-Of-India-With-Respect-To-Time-Series-Effect-And-Performance-Of-Sovereign-Gold-Bond.pdf

86. T. Arumugam, K. M. Ashifa, V. Vinayagalakshmi, U. Kiran, and S. Ramya, "Big Data in Driving Greener Social Welfare and Sustainable Environmental Management," Advances in Business Information Systems and Analytics Book Series, pp. 328–343, Dec. 2023.

87. T. Arumugam, M. A. Sanjeev, R. K. Mathai, S. R. Boselin Prabhu, R. Balamourougane, and T. Jarin, "An empirical verification of the proposed distributor marketing intelligence system model," International Journal of Business Information Systems, vol. 45, no. 4, pp. 454–473, Jan. 2024.

88. T. Arumugam, R. Arun, R. Anitha, P. L. Swerna, R. Aruna, and V. Kadiresan, "Advancing and methodizing artificial intelligence (AI) and socially responsible efforts in real estate marketing," Advances in Business Information Systems and Analytics Book Series, pp. 48–59, Dec. 2023.

89. T. Arumugam, R. Arun, S. Natarajan, K. K. Thoti, P. Shanthi, and U. K. Kommuri, "Unlocking the Power of Artificial Intelligence and Machine Learning in Transforming Marketing as We Know It," Advances in Business Information Systems and Analytics Book Series, pp. 60–74, Dec. 2023.

90. T. Arumugam, R. Mathai, K. Balasubramanian, Renuga K., M. Rafiq, and V. Kalyani, "The mediating effect of customer intimacy on electronic word of mouth (eWOM) in social networking sites on buying intention," Zenodo (CERN European Organization for Nuclear Research), Sep. 2021.

91. T. Arumugam, S. Sethu, V. Kalyani, S. S. Hameed, and P. Divakar, "Representing women entrepreneurs in Tamil movies," The American Journal of Economics and Sociology, vol. 81, no. 1, pp. 115–125, Jan. 2022.

92. T. Arumugam, S. Shahul Hameed, and M. A. Sanjeev, "Buyer behaviour modelling of rural online purchase intention using logistic regression," International Journal of Management and Enterprise Development, vol. 22, no. 2, pp. 139–139, Jan

93. Thangaraja, "An evolution of distributors' marketing intelligence system (DMIS) among FMCG distributors: A conceptual frame work," International Journal of Multidisciplinary Education and Research, vol. 1, no. 5, pp. 11–13, Jul. 2016.

94. U. K. Kommuri and T. Arumugam, "Greenwashing Unveiled: How It Impacts Stakeholder Perception as well as Sustainability Realities," Shanlax International Journal of Arts Science and Humanities, vol. 11, no. S3-Feb, pp. 96–101, Feb. 2024.

95. V. Kadiresan, T. Arumugam, M. Selamat, and B. Parasuraman, "Pull factors, career anchor and turnover of academicians in Malaysian higher education," Journal of International Business and Economics, vol. 16, no. 4, pp. 59–80, Oct. 2016.

96. V. Kadiresan, T. Arumugam, N. Jayabalan, A. R. H. Binti, and C. Ramendran SPR, "HR practices and employee retention. Leader-Member Exchange (LMX) as a mediator," International Journal of Engineering and Advanced Technology, vol. 8, no. 6S3, pp. 618–622, Nov. 2019.

97. A. Kure, S. G. Konda, S. S. Chobe, G. G. Mandawadand B. S. Hote, "Four Component One Pot Synthesis of Benzyl Pyrazolyl Coumarin Derivatives Catalyzed by Metal-Free, Heterogeneous Chitosan Supported Ionic Liquid Carbon Nanotubes", Jan. 2023.

98. B. S. Dawane, B. M. Shaikh, N. T. Khandare, V. T. Kamble, S. S. Chobeand S. G. Konda, "Eco-friendly polyethylene glycol-400: a rapid and efficient recyclable reaction medium for the synthesis of thiazole derivatives", vol. 3, no. 3, Oct. 2010.

99. M. Haroun, "1,5-Benzothiazepine Derivatives: Green Synthesis, In Silico and In Vitro Evaluation as Anticancer Agents", vol. 27, no. 12, Jun. 2022.

100. S. D. Beedkar, C. N. Khobragade, S. S. Chobe, B. S. Dawaneand O. S. Yemul, “Novel thiazolo-pyrazolyl derivatives as xanthine oxidase inhibitors and free radical scavengers.”, vol. 50, no. 4, May 2012.

101. S. G. Konda, S. S. Chobe, A. Gosar, B. S. Hoteand G. G. Mandawad, “Polyethylene glycol-400 Prompted An Efficient Synthesis of Thienyl Pyrazolo[1,5-a] pyrimidines as Microbial Inhibitors”, vol. 19, no. 6, Mar. 2022.

102. S. S. Chobe, “Green approach towards synthesis of substituted pyrazole-1,4-dihydro,9-oxa,1,2,6,8-tetrazacyclopentano[b]naphthalene-5-one derivatives as antimycobacterial agents”, vol. 22, no. 11, Feb. 2013.

103. S. S. Chobe, B. S. Dawane, K. M. Tumbi, P. P. Nandekarand A. T. Sangamwar, “An ecofriendly synthesis and DNA binding interaction study of some pyrazolo [1,5-a]pyrimidines derivatives”, vol. 22, no. 24.

104. B. Verma, A. Srivastava, R. Mehta, Meenakshi and J. Chandel, "FDI-linked Spillovers and the Indian Economic Growth: The role of Country's Absorptive Capacity," 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 2022, pp. 1-6.

105. Verma, B., & Srivastava, A. (2022). Dimensions of globalisation and economic growth of India: exploring causal linkages. International Journal of Economic Policy in Emerging Economies, 15(2-4), 197-213.

106. Verma, B., & Srivastava, D. A. (2020). A Comparative Analysis of Effect of Different Measures of Globalization on Economic Development. International Journal of Development and Conflict, 10, 246-264.

107. V. P. K. Kaluvakuri, “Revolutionizing Fleet Accident Response with AI: Minimizing Downtime, Enhancing Compliance, and Transforming Safety,” SSRN Electronic Journal, Feb. 2023.

108. V. P. K. Kaluvakuri, “AI-Powered continuous deployment: achieving zero downtime and faster releases,” SSRN Electronic Journal, Sep. 2023.

109. V. P. K. Kaluvakuri, “AI-Driven fleet financing: transparent, flexible, and upfront pricing for smarter decisions,” SSRN Electronic Journal, Dec. 2022.

110. V. P. K. Kaluvakuri, V. P. Peta, and S. K. R. Khambam, “Serverless Java: A performance analysis for Full-Stack AI-Enabled Cloud applications,” SSRN Electronic Journal, May. 2021.

111. V. P. K. Kaluvakuri, S. K. R. Khambam, and V. P. Peta, “AI-Powered Predictive Thread Deadlock Resolution: An intelligent system for early detection and prevention of thread deadlocks in cloud applications,” SSRN Electronic Journal, Sep. 2021.

112. S. Banala, Identity and Access Management in the Cloud, International Journal of Innovations in Applied Sciences & Engineering, vol. 10, no. 1S, pp. 60–69, 2024.

113. S. Banala, "The FinOps Framework: Integrating Finance and Operations in the Cloud," International Journal of Advances in Engineering Research, vol. 26, no. 6, pp. 11–23, 2024.

114. S. Banala, "Artificial Creativity and Pioneering Intelligence: Harnessing Generative AI to Transform Cloud Operations and Environments," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no. 1, pp. 34–40, 2023.

115. S. Banala, Cloud Sentry: Innovations in Advanced Threat Detection for Comprehensive Cloud Security Management, International Journal of Innovations in Scientific Engineering, vol. 17, no. 1, pp. 24–35, 2023.

116. S. Banala, Exploring the Cloudscape - A Comprehensive Roadmap for Transforming IT Infrastructure from On-Premises to Cloud-Based Solutions, International Journal of Universal Science and Engineering, vol. 8, no. 1, pp. 35–44, 2022.

117. J. Kaur, P. Mishra, P. Singh, "Hand and Mobile Gesture-Controlled Robot," Grenze International Journal of Engineering & Technology (GIJET), vol. 10, 2024.

118. J. Kaur, A. Gupta, A. Tripathi, A. K. Gupta, A. Srivastava, "RaktFlow: Blood Bank Management and Donation System," in 2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON), 2023, pp. 1-6.

119. J. Chawla, A. K. Ahlawat, "Analysis and Performance of JADE on Interoperability Issues between Two Platform Languages," presented at the 2nd Congress on Intelligent Systems (CIS 2021), organized by Soft Computing Research Society, CRIST, Bengaluru, 2021.

120. J. Chawla, A. K. Ahlawat, G. Goswami, "Integrated Architecture of Web Services Using Multiagent System for Minimizing Interoperability," presented at the 6th International Conference on Computing for Sustainable Global Development, 13th-15th March 2019, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi, India.

121. P. P. Anand, U. K. Kanike, P. Paramasivan, S. S. Rajest, R. Regin, and S. S. Priscila, "Embracing Industry 5.0: Pioneering Next-Generation Technology for a Flourishing Human Experience and Societal Advancement," FMDB Transactions on Sustainable Social Sciences Letters, vol.1, no. 1, pp. 43–55, 2023.

122. G. Gnanaguru, S. S. Priscila, M. Sakthivanitha, S. Radhakrishnan, S. S. Rajest, and S. Singh, "Thorough analysis of deep learning methods for diagnosis of COVID-19 CT images," in Advances in Medical Technologies and Clinical Practice, IGI Global, pp. 46–65, 2024.

123. G. Gowthami and S. S. Priscila, "Tuna swarm optimisation-based feature selection and deep multimodal-sequential-hierarchical progressive network for network intrusion detection approach," Int. J. Crit. Comput.-based Syst., vol. 10, no. 4, pp. 355–374, 2023.

124. A. J. Obaid, S. Suman Rajest, S. Silvia Priscila, T. Shynu, and S. A. Ettyem, "Dense convolution neural network for lung cancer classification and staging of the diseases using NSCLC images," in Proceedings of Data Analytics and Management, Singapore; Singapore: Springer Nature, pp. 361–372, 2023.

125. S. S. Priscila and A. Jayanthiladevi, "A study on different hybrid deep learning approaches to forecast air pollution concentration of particulate matter," in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023.

126. S. S. Priscila, S. S. Rajest, R. Regin, and T. Shynu, "Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm," Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.

127. S. S. Priscila and S. S. Rajest, "An Improvised Virtual Queue Algorithm to Manipulate the Congestion in High-Speed Network"," Central Asian Journal of Medical and Natural Science, vol. 3, no. 6, pp. 343–360, 2022.

128. S. S. Priscila, S. S. Rajest, S. N. Tadiboina, R. Regin, and S. András, "Analysis of Machine Learning and Deep Learning Methods for Superstore Sales Prediction," FMDB Transactions on Sustainable Computer Letters, vol. 1, no. 1, pp. 1–11, 2023.

129. R. Regin, Shynu, S. R. George, M. Bhattacharya, D. Datta, and S. S. Priscila, "Development of predictive model of diabetic using supervised machine learning classification algorithm of ensemble voting," Int. J. Bioinform. Res. Appl., vol. 19, no. 3, 2023.

130. S. Silvia Priscila, S. Rajest, R. Regin, T. Shynu, and R. Steffi, “Classification of Satellite Photographs Utilizing the K-Nearest Neighbor Algorithm,” Central Asian Journal of Mathematical Theory and Computer Sciences, vol. 4, no. 6, pp. 53–71, 2023.

131. S. S. Rajest, S. Silvia Priscila, R. Regin, T. Shynu, and R. Steffi, “Application of Machine Learning to the Process of Crop Selection Based on Land Dataset,” International Journal on Orange Technologies, vol. 5, no. 6, pp. 91–112, 2023.

132. T. Shynu, A. J. Singh, B. Rajest, S. S. Regin, and R. Priscila, “Sustainable intelligent outbreak with self-directed learning system and feature extraction approach in technology,” International Journal of Intelligent Engineering Informatics, vol. 10, no. 6, pp.484-503, 2022.

133. S. S. Priscila, D. Celin Pappa, M. S. Banu, E. S. Soji, A. T. A. Christus, and V. S. Kumar, “Technological frontier on hybrid deep learning paradigm for global air quality intelligence,” in Cross-Industry AI Applications, IGI Global, pp. 144–162, 2024.

134. S. S. Priscila, E. S. Soji, N. Hossó, P. Paramasivan, and S. Suman Rajest, “Digital Realms and Mental Health: Examining the Influence of Online Learning Systems on Students,” FMDB Transactions on Sustainable Techno Learning, vol. 1, no. 3, pp. 156–164, 2023.

135. S. R. S. Steffi, R. Rajest, T. Shynu, and S. S. Priscila, “Analysis of an Interview Based on Emotion Detection Using Convolutional Neural Networks,” Central Asian Journal of Theoretical and Applied Science, vol. 4, no. 6, pp. 78–102, 2023.