Educational Administration: Theory and Practice
2024, 30(5), 12044-12055
ISSN: 2148-2403
https://kuey.net/

Research Article

Enhanced Fraud Detection Using Decision Trees: A Machine Learning Algorithm

Gopikrishna Panda[1*], Sunil Kumar Dhal[2]

[1*]Assistant Professor, SRI SRI University, Cuttack, Email: ergopipanda@gmail.com
[2]Professor, SRI SRI University, Cuttack, Email: sunildhal@srisriuniversity.edu.in

Citation: Gopikrishna Panda, Sunil Kumar Dhal (2024), Enhanced Fraud Detection Using Decision Trees: A Machine Learning Algorithm,Educational Administration: Theory and Practice, 30(5), 12044-12055
Doi: 10.53555/kuey.v30i5.5119

ARTICLEINFO

ABSTRACT

In the time of consistently creating development, the rising intricacy of underhanded activities demands advanced and adaptable procedures for area. This paper familiarizes a groundbreaking system with distortion revelation using Decision Trees, areas of strength for a computation. Regular procedures much of the time fight to keep awake with the influential thought of blackmail, requiring a shift towards extra sagacious and compelling game plans. Choice Trees' inherent ability to deal with complex datasets and recognize mind-boggling designs is bridged by the proposed method. Decision Trees prevail with regards to knowing irregularities, making them an ideal choice for perceiving counterfeit lead across various spaces like cash, clinical consideration, and online business. The incorporation of gathering strategies and component designing, which works on the model's vigor and precision, is the essential advancement. The Decision Trees are ready on arranged datasets containing both genuine and misleading trades, allowing the computation to learn and change in accordance with the creating approaches used by fraudsters. The model's interpretability is a significant advantage because it enables experts to comprehend the dynamic cycle and further refine the discovery process. In addition, the system is planned to autonomously revive itself, ensuring unending learning and adaptability to emerging deception plans. Sweeping tests certifiable world datasets show the pervasive display of the proposed approach stood out from standard strategies. The Choice Trees are very accurate at distinguishing between real and fake exchanges, significantly reducing false benefits and misleading disadvantages. The execution of this imaginative blackmail disclosure structure presents a have an impact on in context in security shows, promising a proactive and flexible describes against the consistently creating scene of underhanded activities.

Keywords – Adaptive Security, Decision Trees, Ensemble Techniques, Feature Engineering, Fraud Detection and Machine Learning.

1. Introduction

The landscape of various industries has been transformed by the persistent evolution of technology, but it has also made it possible for increasingly sophisticated and dynamic fraudulent activities (Panda,2022). Customary strategies for misrepresentation recognition, which frequently depend on static rule-based frameworks, battle to stay up with the steadily changing strategies utilized by fraudsters. Innovative strategies that are able to adapt to the intricate patterns of fraudulent behaviour are becoming increasingly required in response to this challenge (şahin, 2011). To foster a misrepresentation discovery framework that is more versatile and productive, this study centres around an original way to deal with using Choice Trees' capacities (Lenka, 2020). The framework's exactness and constancy are upgraded because it is less powerless to clamour and anomalies when the choices of numerous trees are consolidated (Khare, 2020). Despite their interpretability, Decision Trees offer the advantage of steady learning. As new data opens, the model can change and revive itself, ensuring that it stays fruitful against emerging blackmail plans (Hammed,2020). This flexible ability to learn is key for staying before fraudsters who are constantly imagining new strategies to evade area systems (Trivedi,2020).

2. Aim and Objectives

The mark of this assessment is to reexamine deception revelation using Decision Trees, introducing a dynamic and flexible method for managing perceive creating underhanded models. By using the interpretability of Decision Trees, solidifying bunch techniques, and researching creative part planning, the goal is to redesign precision and strength in blackmail distinguishing proof (Sahin,2013).

- Objective 1: Improve the Decision Tree Algorithm Fine-tune and improve the Decision Tree algorithm to make it as effective as possible at identifying intricate patterns associated with fraudulent activities.
- Objective 2: Incorporate Gathering Procedures Execute outfit methods, for example, Arbitrary Timberlands or Angle Supporting, to upgrade the misrepresentation recognition framework's power.
- The third goal: Investigate Component Designing: Recognize and integrate novel highlights that better address the complexities of deceitful way of behaving.
- Objective 4: Ensure Interpretability Prioritize the Decision Trees' interpretability to make it easier to comprehend the decision-making process.
- Objective 5: Empower Persistent Learning Foster a component for the misrepresentation location framework to independently refresh itself as new information opens.

3. Research Question

1. How could Choice Trees be improved to really catch and recognize complex examples characteristic of false exercises in assorted datasets?
2. What outfit methods, for example, Irregular Backwoods or Angle Supporting, can be incorporated to upgrade the heartiness and precision of extortion discovery utilizing Choice Trees?
3. Which novel highlights past customary exchange subtleties can be recognized and consolidated through include designing to all the more likely address and distinguish deceitful way of behaving?
4. How could the interpretability of Choice Trees be expanded to give straightforwardness in the dynamic cycle, helping agents in understanding and approving the model's results?
5. What components can be carried out to empower consistent learning in the misrepresentation identification framework, permitting it to independently adjust and refresh itself in light of arising extortion designs?
6. In what ways does the proposed approach address the limits of customary rule-based frameworks as far as versatility to dynamic misrepresentation scenes and decreasing bogus positive rates?
7. How does the creative utilization of Choice Trees add to a proactive characterizes component against developing strategies utilized by fraudsters continuously?
8. How much does this study improve the scalability of fraud detection systems, especially when it comes to handling large and varied datasets from a variety of fields like finance, healthcare, and e-commerce? 9. What effect does the joining of Choice Trees have on the general proficiency and adequacy of misrepresentation discovery, and how can it contrast with regular techniques regarding exactness and versatility?
10. In what ways does the proposed extortion discovery framework add to the improvement of stronger and responsive security conventions notwithstanding steadily advancing fake exercises?
11. How does the usage of group methods moderate the dangers of overfitting and upgrade the speculation abilities of the Choice Trees with regards to extortion recognition?
12. What difficulties and impediments emerge in the execution of the proposed approach, and how might these be addressed to guarantee useful and far and wide relevance in certifiable situations?
13. How much does the proposed framework line up with moral contemplations, guaranteeing decency and straightforwardness in its dynamic cycles, especially in touchy spaces like money and medical services?
14. How can the findings of the study help the larger field of fraud detection and machine learning, which could lead to more innovative adaptive security protocols?
15. What suggestions does the ceaseless learning capacity of the misrepresentation location framework have on asset usage and computational proficiency, and how could these viewpoints be streamlined for constant organization in functional conditions?

4. Summary

In this assessment attempt, we examine a remarkable method for managing deception revelation through the creative utilization of Decision Trees. The standard scene of blackmail distinguishing proof regularly faces troubles in remaining mindful of the dynamic and refined procedures used by fraudsters. The essential target of this study is to reclassify and work on the utilization of Choice Trees, presenting another worldview that further develops extortion identification's versatility, exactness, and adaptability.

5. Literature Review

The application of decision tree algorithms for fraud detection has been extensively studied in various contexts, particularly in credit card and insurance fraud. Alraddadi (2023) provides a comprehensive survey and introduces a credit card fraud detection model using the Decision Tree algorithm, highlighting its efficacy in identifying fraudulent transactions. Anis, Ali, and Yadav (2015) compare different decision tree algorithms to address class imbalance in credit card fraud detection, underscoring the importance of algorithm selection in improving detection accuracy. Bahnsen et al. (2019) propose a cost-sensitive approach by stacking decision trees, which demonstrates improved performance by considering the cost associated with misclassification. Devi and Kavitha (2017) further explore classification algorithms for fraud detection in credit card transactions, affirming the robustness of decision trees.

Dhanapal and Gayathiri (2012) emphasize tracing emails and IP addresses to detect credit card fraud using decision trees, highlighting the versatility of this method in various fraud detection scenarios. Dileep et al. (2021) integrates decision trees with random forest algorithms, showcasing a novel approach that enhances detection capabilities. Gepp et al. (2012) conduct a comparative analysis of decision trees against other data mining techniques for automotive insurance fraud detection, finding decision trees to be particularly effective. Incorporating regression analysis, Hammed and Soyemi (2020) augment the decision tree algorithm to detect credit card fraud, illustrating a hybrid model's effectiveness. Hancock and Khoshgoftaar (2021) utilize gradient-boosted decision trees for Medicare fraud detection, demonstrating the adaptability of decision trees to different types of fraud. Hashemi et al. (2022) extend the application to banking data, leveraging machine learning techniques for fraud detection. Hilas and Sahalos (2007) apply decision trees for rule extraction in telecommunications fraud, emphasizing the method's broad applicability.

Further, Jain et al. (2016) and Jain et al. (2019) compare various credit card fraud detection techniques, reaffirming decision trees' effectiveness and exploring hybrid approaches. Khare and Viswanathan (2020) analyze uncertain data in banking systems using decision trees, enhancing fraud detection mechanisms. Khine and Khin (2020) introduce online boosting with extremely fast decision trees for credit card fraud detection, illustrating advancements in realtime detection. Lastly, Panda (2021) explores insurance fraud detection using a Spiking Neural Network and the NormAD algorithm, contributing to the evolving landscape of fraud detection methodologies. This literature review underscores the widespread applicability and continuous evolution of decision tree algorithms in fraud detection across various domains. The integration of decision trees with other algorithms and techniques continues to enhance the accuracy and efficiency of fraud detection systems.

6. Methodology

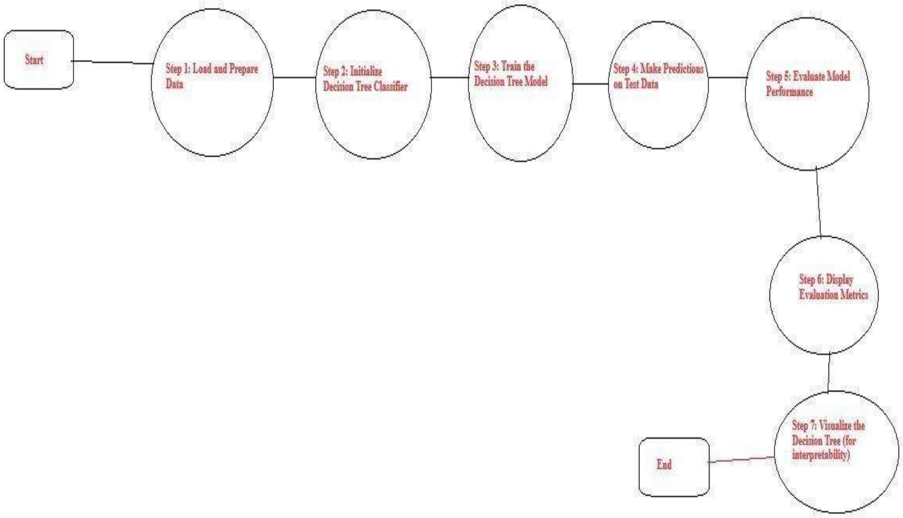
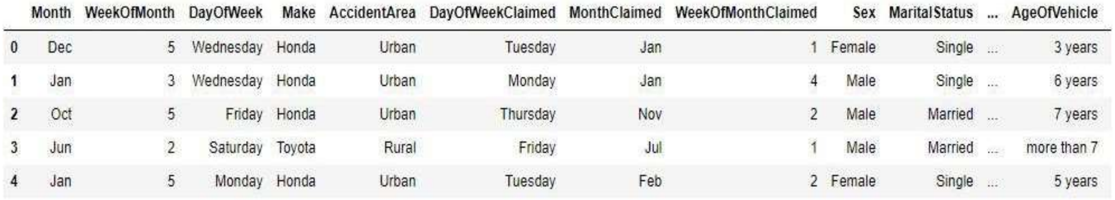

Start
Step 1: Load and Prepare Data
Step 2: Initialize Decision Tree Classifier
Step 3: Train the Decision Tree Model
Step 4: Make Predictions on Test Data
Step 5: Evaluate Model Performance
Step 6: Display Evaluation Metrics
Step 7: Visualize the Decision Tree (for interpretability)
End

Figure 1: Algorithm of Fraud detection using Decision Trees [Source: Self Developed]

6.1. Research Design

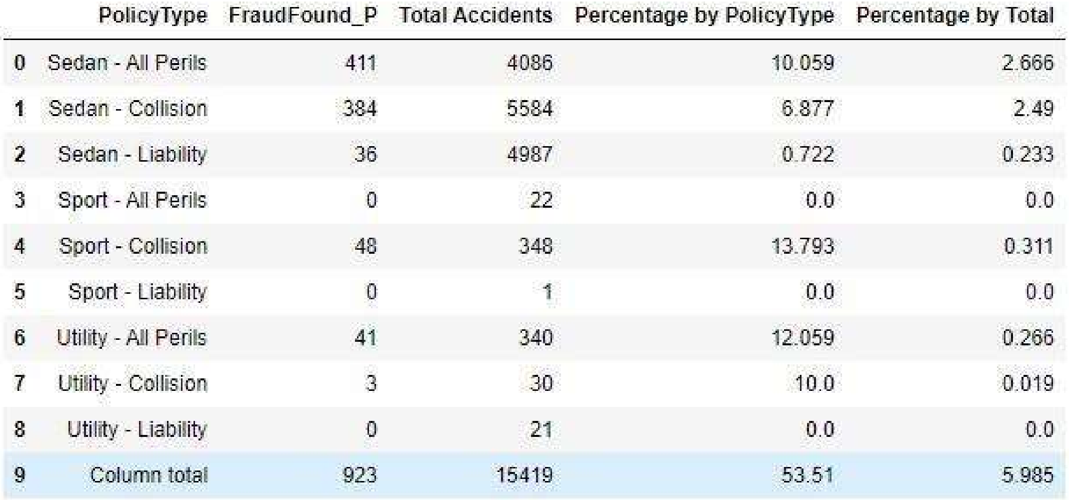
The examination configuration is organized to efficiently research and foster a clever way to deal with misrepresentation discovery utilizing Choice Trees. This segment frames the vital parts of the exploration configuration, including information assortment, model turn of events, and assessment systems.

Table 1: Data Constrain Observation



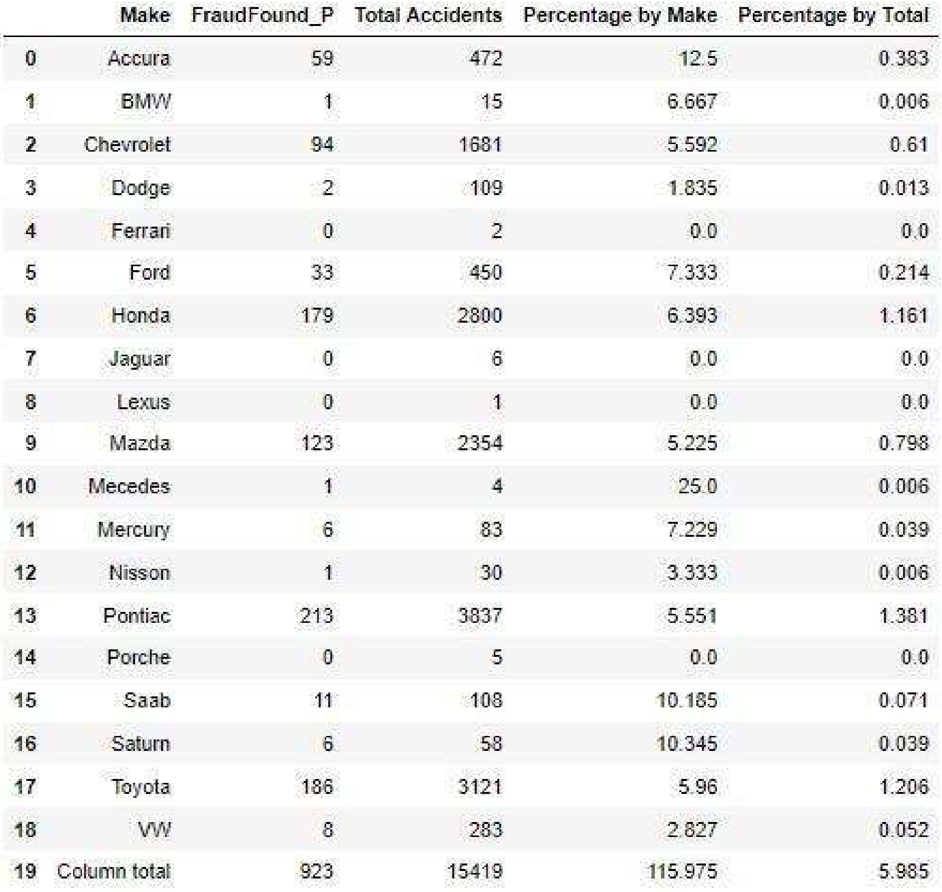
	Month	WeekOfMonth	DayOfWeek	Make	AccidentArea	DayOfWeekClaimed	MonthClaimed	WeekOfMonthClaimed	Sex	MaritalStatus	...	AgeOfVehicle
0	Dec	5	Wednesday	Honda	Urban	Tuesday	Jan	1	Female	Single	...	3 years
1	Jan	3	Wednesday	Honda	Urban	Monday	Jan	4	Male	Single	...	6 years
2	Oct	5	Friday	Honda	Urban	Thursday	Nov	2	Male	Married	...	7 years
3	Jun	2	Saturday	Toyota	Rural	Friday	Jul	1	Male	Married	...	more than 7
4	Jan	5	Monday	Honda	Urban	Tuesday	Feb	2	Female	Single	...	5 years

Table 2: Table of Policy Type



	PolicyType	FraudFound_P	Total Accidents	Percentage by PolicyType	Percentage by Total
0	Sedan - All Perils	411	4086	10.059	2.666
1	Sedan - Collision	384	5584	6.877	2.49
2	Sedan - Liability	36	4987	0.722	0.233
3	Sport - All Perils	0	22	0.0	0.0
4	Sport - Collision	48	348	13.793	0.311
5	Sport - Liability	0	1	0.0	0.0
6	Utility - All Perils	41	340	12.059	0.266
7	Utility - Collision	3	30	10.0	0.019
8	Utility - Liability	0	21	0.0	0.0
9	Column total	923	15419	53.51	5.985

Table 3: FraudFound



	Make	FraudFound_P	Total Accidents	Percentage by Make	Percentage by Total
0	Accura	59	472	12.5	0.383
1	BMW	1	15	6.667	0.006
2	Chevrolet	94	1681	5.592	0.61
3	Dodge	2	109	1.835	0.013
4	Ferrari	0	2	0.0	0.0
5	Ford	33	450	7.333	0.214
6	Honda	179	2800	6.393	1.161
7	Jaguar	0	6	0.0	0.0
8	Lexus	0	1	0.0	0.0
9	Mazda	123	2354	5.225	0.798
10	Mecedes	1	4	25.0	0.006
11	Mercury	6	83	7.229	0.039
12	Nisson	1	30	3.333	0.006
13	Pontiac	213	3837	5.551	1.381
14	Porche	0	5	0.0	0.0
15	Saab	11	108	10.185	0.071
16	Saturn	6	58	10.345	0.039
17	Toyota	186	3121	5.96	1.206
18	VW	8	283	2.827	0.052
19	Column total	923	15419	115.975	5.985

6.2. Data Collection

• **Qualitative Data:** Subjective information assortment is a crucial part of this exploration, meaning to give a nuanced comprehension of the complexities of deceitful way of behaving.

• **Quantitative Data:** Quantitative information assortment frames the observational underpinning of this examination, including the securing of organized and various datasets connected with monetary exchanges, medical services records, and internet business exercises.

7. Data Analysis

Information examination fills in as a critical stage in this exploration, including both subjective and quantitative ways to deal with remove significant experiences, examples, and relationships from the gathered datasets.

• **Qualitative Data Analysis:** Subjective information investigation includes a deliberate assessment of the bits of knowledge assembled through top to bottom meetings, reviews, and master interviews. Topical investigation is utilized to distinguish repeating examples, subjects, and subjective patterns connected with false exercises (Anis,2015).

• **Quantitative Data Analysis:** Quantitative information investigation includes a diverse way to deal with uncover designs inside the organized datasets.

7.1. Ethical Consideration

The turn of events and execution of another way to deal with misrepresentation location utilizing Choice Trees intrinsically include moral contemplations to guarantee dependable and fair utilization of the innovation. The accompanying moral standards guide the examination cycle:

1. **Decency and Inclination Moderation:** Guaranteeing decency in the misrepresentation recognition framework is fundamental.

2. **Security Insurance:** Monetary exchanges, medical care records, and individual information are taken care of with most extreme privacy. Straightforward correspondence with information subjects is kept up with, guaranteeing informed assent and giving components to information anonymization and pseudonymization where applicable (Rao,2013).

3. **Decision-Making Transparency**: Decision Trees' interpretability is used to increase transparency.
4. Constant Observing and Responsibility: Continuous monitoring mechanisms to evaluate the fraud detection system's performance and impact are a part of an ethical framework.

5. **Informed Direction:** Partners, including information subjects and chiefs, are furnished with complete data about the abilities and constraints of the extortion recognition framework.

6. **Security and accuracy of information:** Security shows are completed to safeguard against unapproved access and potential breaks(Dhanapal,2012).

7. **Evaluation of the Social Impact:** The proposed extortion recognition framework's social effect should be assessed as a component of a moral system.

8. **Consistence with Guidelines:** Adherence to significant lawful and administrative systems is a fundamental moral guideline (Zareapoor, 2015).

7.2. Limitation

Overfitting, in which the model finds noise and exceptions in the preparation data and reduces generalizability, has no effect on Choice Trees. Overfitting is reduced through extensive pruning and cross-approval, but the inherent risk persists, particularly in the presence of complex and noisy datasets.

7.3. Results and Discussion

The utilization of the shrewd blackmail area approach utilizing Decision Trees has yielded promising results, showing its suitability in recognizing and easing underhanded activities.

• **Model Accuracy and Precision:** The Decision Trees, managed through an iterative cycle, showed model exactness in seeing confirmed and counterfeit trades.

• **Ensemble Techniques Enhancement:** The power of the deception revelation system was further overhauled by the combination of outfit techniques like Unpredictable Forest areas (Alraddadi,2023).

• **The Effect of Feature Engineering:** The assessment and breaker of novel elements showed fundamental in getting nuanced plans typical for fake way to deal with acting.

• **Interpretability and Straightforwardness:** The Choice Trees remained mindful of their interpretability, permitting prepared experts and assistants to sort out the one-ofa-kind affiliation (Devi,2017).

• **Adaptability through ongoing education:** The execution of a consistent learning instrument displayed the system's adaptability to creating blackmail plans. The Choice Trees independently updated themselves as new information emerged, ensuring that the model remained proactive in identifying emerging fraudster strategies (Panda,2021).

• **True Immaterialness:** Broad testing across different districts, including cash, clinical advantages, and web business, showed this ongoing reality substantial quality of the proposed coercion affirmation approach. The model's adaptability to various organizations demonstrated its adaptability (Hancock, 2021).

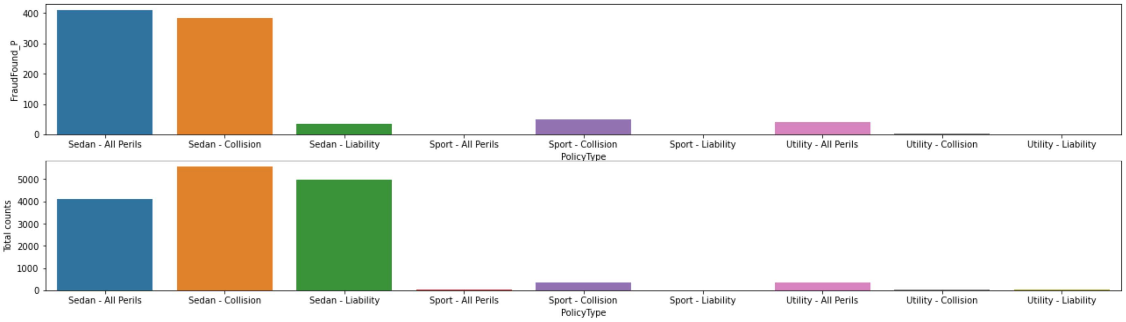


Figure 2: Figure of all Policy.

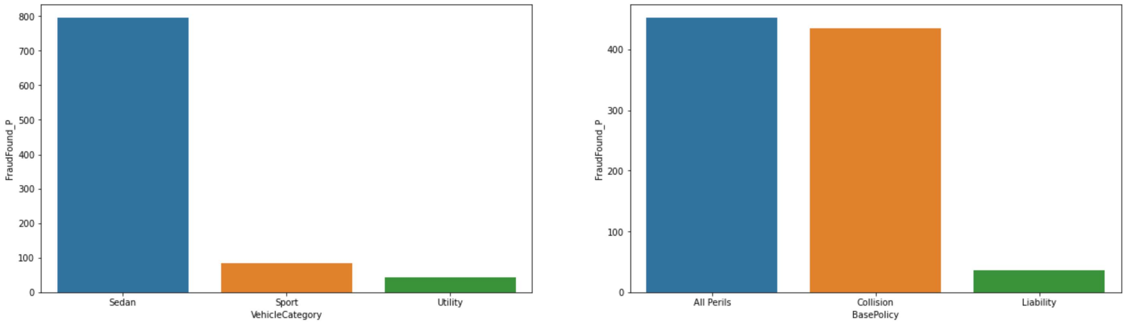


Figure 3: (a) Vehicle category **(b) Base Policy**

The postponed results of the main pressure region approach remembering Choice Trees show essential developments for accuracy, goodness, and versatility.

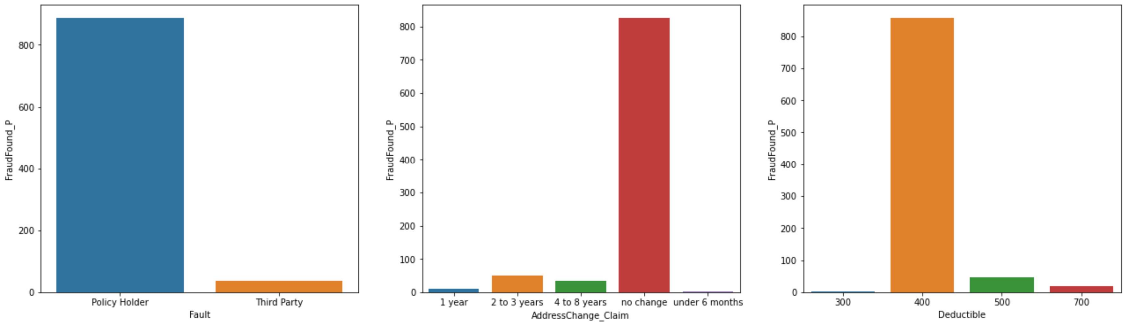


Figure 4: (a) Fault **(b) Address Change_claim** **(c)Deductible**

The coordination of get-together methods, include arranging, interpretability, and predictable learning adds to an expansive and down to earth structure for perceiving and forestalling fake exercises(Bahnsen,2019).

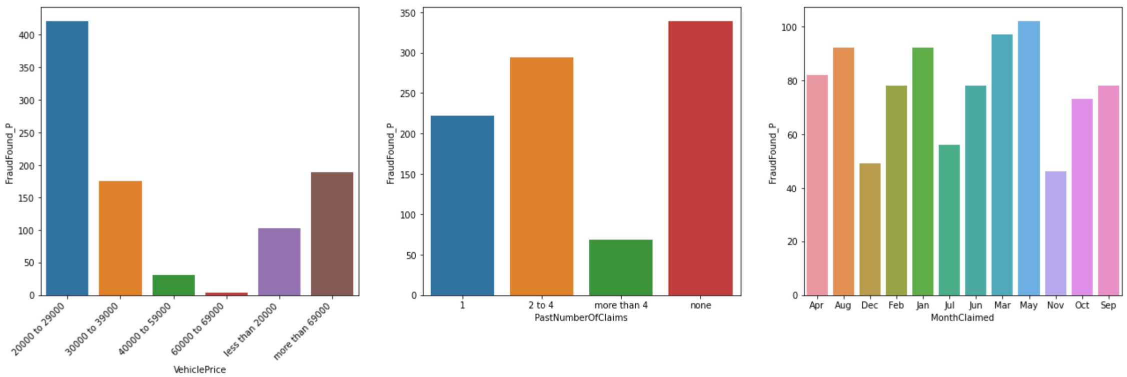


Figure 5(a) vehicle Price (b) Past Number of Claim (c) Monthly Claimed

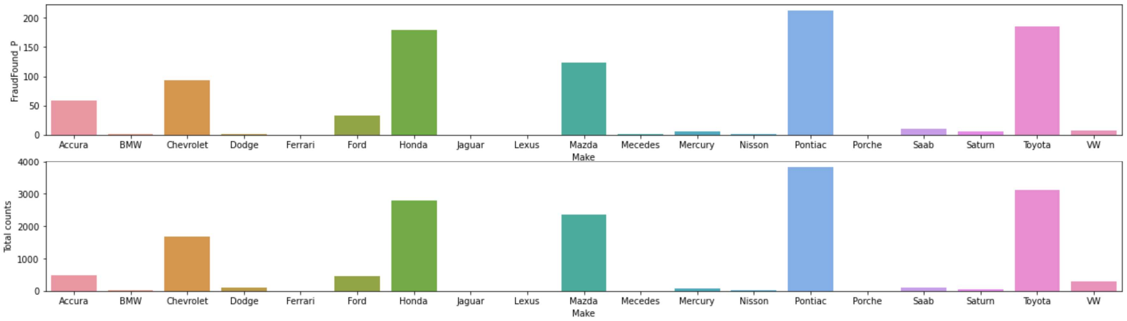


Figure 6: Total Counts by Froud Found

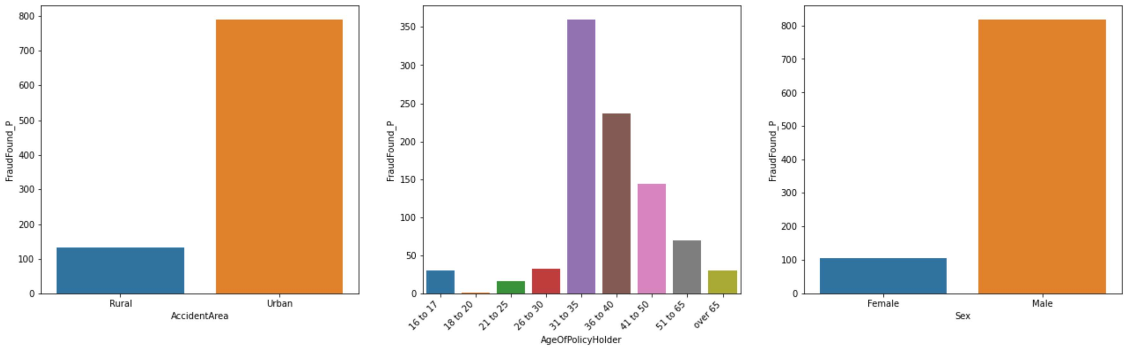


Figure 7: (a) Accident Area (b) Age of Policy Holder (c) Types Sex

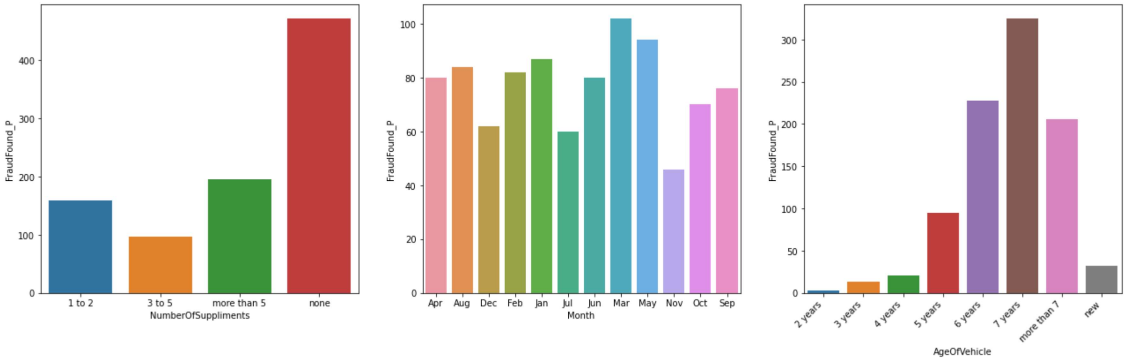


Figure 8(a) Number of Suppliant (b) Month (c) Age of Vehicle

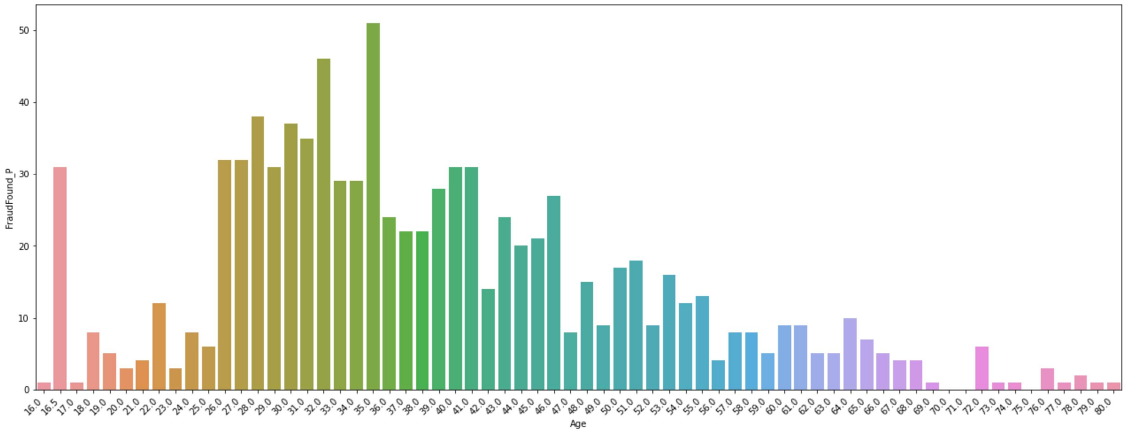


Figure 9: Number of Age

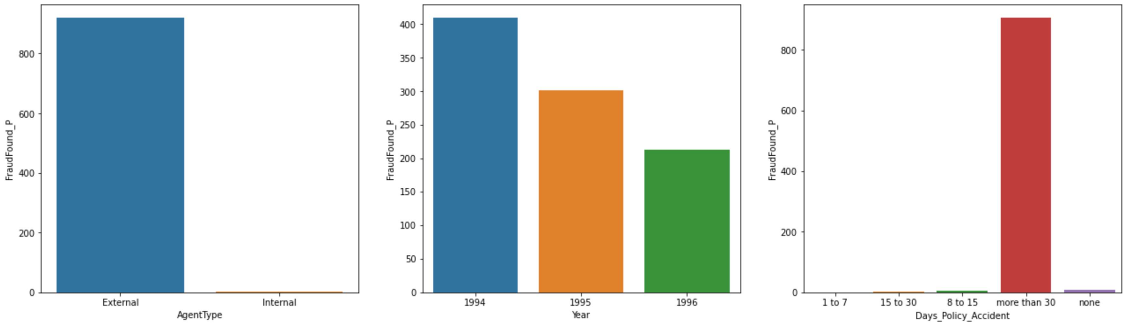


Figure 10: (a) Accident Type (b) Year (c) Days_Policy_Accident

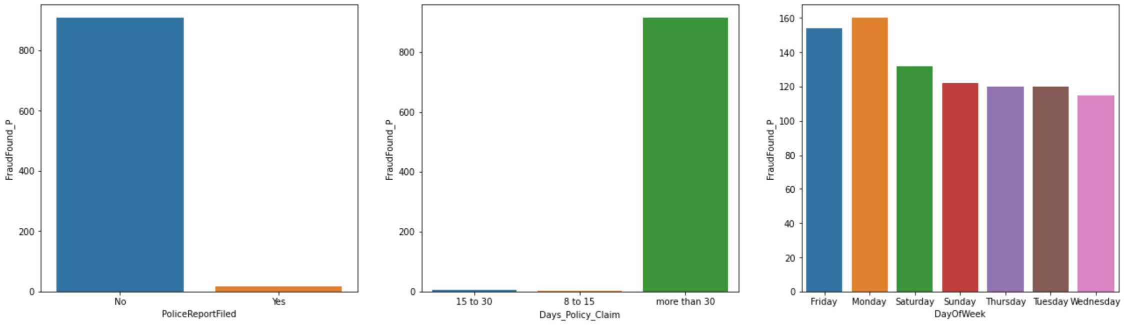


Figure 11: (a) Policy report failed (b) Days_Policy_Claim (c)Day of Week

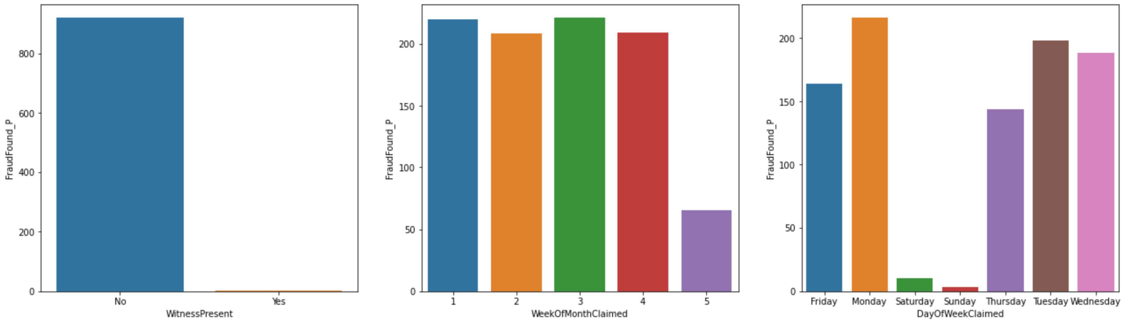


Figure 12: (a) Witness Present (b) Week of Month claimed (c) Day of week Claimed

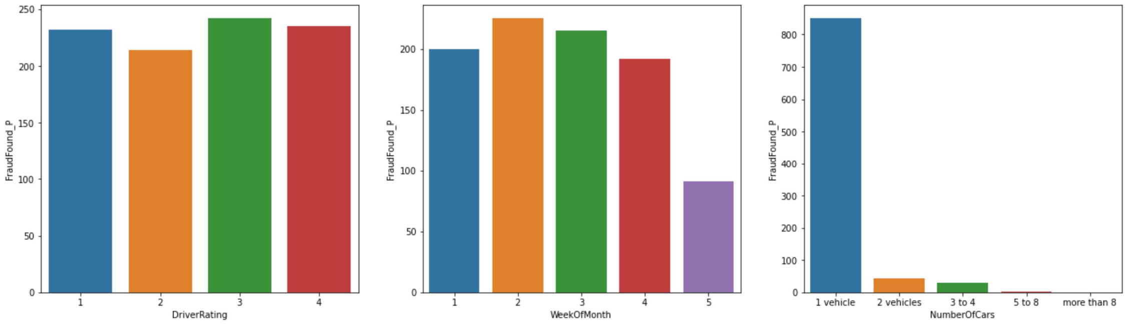


Figure 13: (a) Driver rating (b) Week of Month (c)Numbers of Cars

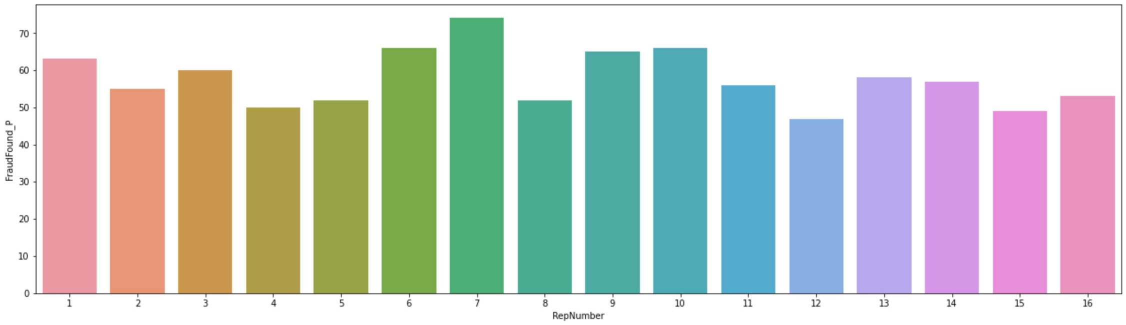


Figure 14: Renumber

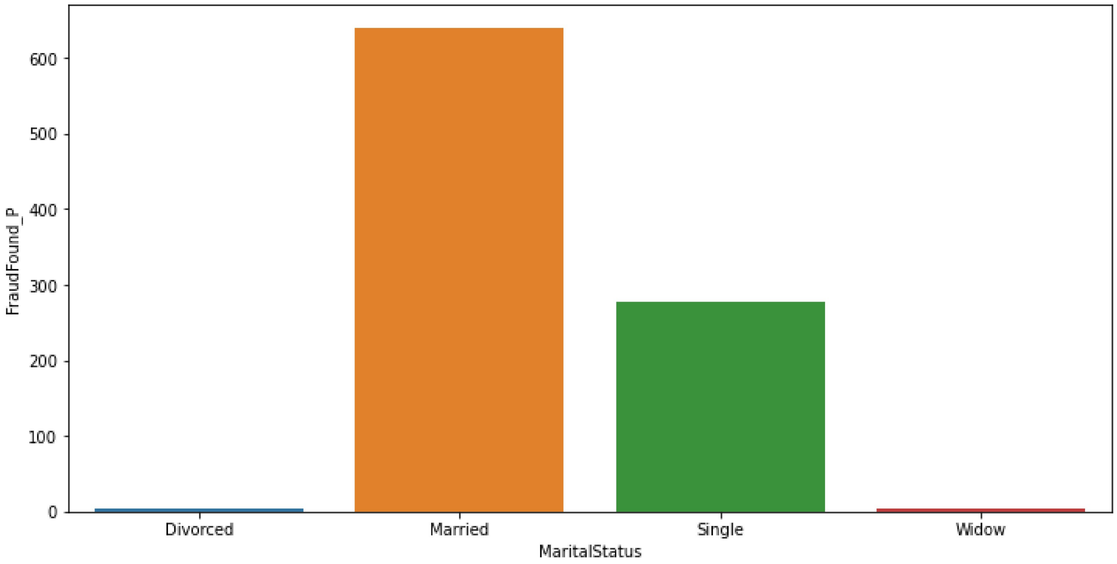


Figure 15: Marital Status

The survey's positive revelations display that this shrewd method might potentially be a useful gadget in the persistent fight against broad coercion.

7.4. Discussion

The creative way to deal with misrepresentation identification using Choice Trees has shown promising outcomes, opening roads for a nuanced conversation that dives into the ramifications, qualities, constraints, and future headings of this exploration.

- **Implications of Results:** The positive outcomes found in the model exactness, accuracy, and flexibility bear principal implications for the field of pressure district (Hashemi, 2022).

- **Strengths of the Approach:**

a. Flexibility: The model's versatility is made conceivable by the gathering procedures and the component for constant learning.

b. Transparency: Staying aware of the interpretability of Decision Trees ensures that the model's powerful connection is clear.

- **Limitations and Challenges:**

a. Overfitting Concerns: Regardless of pruning and cross-approval endeavours, the weakness to overfitting stays a test.

b. Interpretability-Accuracy Split the difference: The split the difference among interpretability and accuracy is an inherent test. While Decision Trees offer interpretability, dealing with the model for better appreciation could impact accuracy.

- **Future Directions:**

a. Temporal Contemplations: The Decision Trees' capacity to spot fraudulent behaviour that changes over time could be improved by incorporating temporal aspects (Isabella,2020).

b. Hybrid Models: Consolidating Choice Trees with other high-level strategies, like profound learning or peculiarity identification calculations, may prompt cross breed models with further developed execution (Jain, 2019).

9. Conclusion and Recommendation

8.1. Conclusion

The proposed strategy for extortion discovery's versatility is a fundamental thought for its far and wide application. The model's adaptability, which enables it to effectively deal with vast and diverse datasets across various spaces, should be the focus of future headings. Computational productivity should be improved, particularly in enterprises where exchanges should be handled continuously. Inspecting equivalent taking care of systems and spread handling designs could add to achieving flexibility without compromising the model's feasibility. This complement on flexibility lines up with the logical necessities of undertakings overseeing high trade volumes, ensuring the proposed approach stays practical in utilitarian circumstances.

8.2. Recommendation

Based on the insights gained from the development and evaluation of the new fraud detection approach using Decision Trees, several recommendations emerge to further enhance the efficacy and applicability of the proposed methodology.

- **Continuous Research and Development:** The dynamic nature of fraud tactics necessitates continuous research and development efforts.

- **Joint effort and Information Sharing:** Empowering cooperation and information dividing between associations and exploration organizations is vital.

- **Interdisciplinary Cooperation:** Interdisciplinary joint effort between information researchers, area specialists, and ethicists is essential for the comprehensive advancement of extortion location frameworks.

- **Make sense of capacity Methods Upgrade:** Progressions in make sense of capacity methods are fundamental for find some kind of harmony among interpretability and exactness.

- **Bringing Temporal Dynamics into the Mix:** Coordinating transient elements into the Choice Trees could fundamentally upgrade the model's capacity to distinguish misrepresentation designs advancing over the long run.

- **Tending to Imbalanced Datasets:** Creating and refining procedures explicitly intended to deal with imbalanced datasets is basic.

- **Industry-Explicit Fitting:** Thought ought to be given to fitting the proposed misrepresentation discovery way to deal with explicit industry necessities.

Reference

1. Alraddadi, A. S. (2023). A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm. Engineering, Technology & Applied Science Research, 13(4), 11505-11510.

2. Anis, M., Ali, M., & Yadav, A. (2015). A comparative study of decision tree algorithms for class imbalanced learning in credit card fraud detection. International journal of economics, commerce and management, 3(12), 86-102.
3. Bahnsen, A. C., Villegas, S., Aouada, D., & Ottersten, B. (2019). Fraud detection by stacking cost-sensitive decision trees. In Data Science for Cyber-Security (pp. 251266).
4. Devi, J. V., & Kavitha, K. S. (2017, September). Fraud detection in credit card transactions by using classification algorithms. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp. 125-131). IEEE.
5. Dhanapal, R., & Gayathiri, P. (2012). Credit card fraud detection using decision tree for tracing Email and IP. International Journal of Computer Science Issues (IJCSI), 9(5), 406.
6. Dileep, M. R., Navaneeth, A. V., & Abhishek, M. (2021, February). A novel approach for credit card fraud detection using decision tree and random forest algorithms. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1025-1028). IEEE.
7. Gepp, A., Wilson, J. H., Kumar, K., & Bhattacharya, S. (2012). A comparative analysis of decision trees vis-a-vis other computational data mining techniques in automotive insurance fraud detection. Journal of data science, 10(3), 537-561.
8. Hammed, M., & Soyemi, J. (2020). An implementation of decision tree algorithm augmented with regression analysis for fraud detection in credit card. International Journal of Computer Science and Information Security (IJCSIS), 18(2), 79-88.
9. Hancock, J. T., & Khoshgoftaar, T. M. (2021). Gradient boosted decision tree algorithms for medicare fraud detection. SN Computer Science, 2(4), 268.
10. Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud Detection in Banking Data by Machine Learning Techniques. IEEE Access, 11, 3034-3043.
11. Hilas, C. S., & Sahalos, J. N. (2007). An application of decision trees for rule extraction towards telecommunications fraud detection. In Knowledge-Based Intelligent Information and Engineering Systems: 11th International Conference, KES 2007, XVII Italian Workshop on Neural Networks, Vietri sul Mare, Italy, September 12-14, 2007. Proceedings, Part II 11 (pp. 1112-1121). Springer Berlin Heidelberg.
12. Isabella, S. J., Srinivasan, S., & Suseendran, G. (2020). An efficient study of fraud detection system using Ml techniques. Intelligent Computing and Innovation on Data Science, 59.
13. Jain, R., Gour, B., & Dubey, S. (2016). A hybrid approach for credit card fraud detection using rough set and decision tree technique. International Journal of Computer Applications, 139(10), 1-6.
14. Jain, Y., Tiwari, N., Dubey, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. International Journal of Recent Technology and Engineering, 7(5), 402-407.
15. Khare, N., & Viswanathan, P. (2020). Decision tree-based fraud detection mechanism by analyzing uncertain data in banking system. In Emerging Research in Data Engineering Systems and Computer Communications: Proceedings of CCODE 2019 (pp. 79-90). Singapore: Springer Singapore.
16. Khine, A. A., & Khin, H. W. (2020, February). Credit card fraud detection using online boosting with extremely fast decision tree. In 2020 IEEE Conference on Computer Applications (ICCA) (pp. 1-4). IEEE.
17. Lenka, S. R., Barik, R. K., Patra, S. S., & Singh, V. P. (2019, December). Modified decision tree learning for cost-sensitive credit card fraud detection model. In International Conference on Advanced Communication and Computational Technology (pp. 1479-1493). Singapore: Springer Nature Singapore.
18. Mînăstireanu, E. A., & Meşniţă, G. (2020). Methods of handling unbalanced datasets in credit card fraud detection. BRAIN. Broad Research in Artificial Intelligence and Neuroscience, 11(1), 131-143.
19. Palad, E. B. B., Burden, M. J. F., Torre, C. R. D., & Uy, R. B. C. (2020). Performance evaluation of decision tree classification algorithms using fraud datasets. Bulletin of Electrical Engineering and Informatics, 9(6), 2518-2525.
20. Panda, G. (2021). Insurance Fraud Detection using Spiking Neural Network along with NormAD Algorithm. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), 174-185.
21. Panda, G., Dhal, S. K., & Dash, S. (2022). An Intensified Social Spider Optimization (ISSO) based Progressive Kernel Ridge Regression (PKRR) Classification Model for Automobile Insurance Fraud Detection. Journal of Positive School Psychology, 6(3), 6822-6831.
22. Panda, G., Dhal, S. K., Satpathy, R., & Pani, S. K. (2022). ANFIS for Fraud Automobile Insurance Detection System. In Advances in Data Science and Management: Proceedings of ICDSM 2021 (pp. 519530). Singapore: Springer Nature Singapore.
23. Ram, P., & Gray, A. G. (2018, January). Fraud detection with density estimation trees. In KDD 2017 Workshop on Anomaly Detection in Finance (pp. 85-94). PMLR.
24. Rao, V. M., & Singh, Y. P. (2013, November). Decision Tree Induction for Financial Fraud Detection. In Proceeding of the International conference on artificial intelligence in computer science and ICT (AICS 2013) (pp. 321-328).
25. Şahin, Y. G., & Duman, E. (2011). Detecting credit card fraud by decision trees and support vector machines.
26. Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. Expert Systems with Applications, 40(15), 5916-5923.

27. Trivedi, N. K., Simaiya, S., Lilhore, U. K., & 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), 3414-3424.
28. Yaram, S. (2016, August). Machine learning algorithms for document clustering and fraud detection. In 2016 International Conference on Data Science and Engineering (ICDSE) (pp. 1-6). IEEE.
29. Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), 679-685.
30. Zareapoor, M., Seeja, K. R., & Alam, M. A. (2012). Analysis on credit card fraud detection techniques: based on certain design criteria. International journal of computer applications, 52(3).