Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

Machine Learning-Based Approaches for Credit Card Fraud Detection: A Comprehensive Review

Dr. K.Maithili¹, Dr. T. Sathish Kumar², Dr. A. Rengarajan³, P L Srinivasa Murthy⁴, K. Nagamani⁵

¹Associate Professor ,Department of CSE KG Reddy College of Engineering &TechnologyMoinabad, Hyderabad, Telangana-501504 Mail: drmaithili@kgr.ac.in

²Associate Professor, Department of Computer Science and Engineering Hyderabad Institute of Technology and Management, Hyderabad . Mail: sathisht.cse@hitam.org

³Professor, Department of CSE, Jain university, Bangalore Mail: a.rengarajan@jainuniversity.ac.in ⁴Professor, Department of Computer science and Engineering, IARE

Mail: plsrinivasamurthy@iare.ac.in

⁵Assistant professor, Department of CSE, MLR Institute of Technology, Dundigal, Hyderabad.

Mail: nagamanik@mlrit.ac.in

Abstract

The objective of data analytics is to discover hidden patterns and use them to guide wise judgements in a range of circumstances. Theft of credit cards has significantly grown as a result of modern technologies and has become a popular target for scam artists. Publicly available databases on credit card fraud are very unbalanced. As more people conduct business online, Fraud involving credit cards has grown to be a serious problem for both consumers and financial establishments, standard rule-based fraud detection strategies have shown to be insufficient to combat fraudsters' ever-evolving tactics. Machine learning algorithms have thus developed into a powerful tool for real-time unsupervised learning, and anomaly detection., is then explored in detail in order to accurately identify fraudulent transactions. Furthermore, we explore the various data features utilized by machine learning algorithms, including transaction history, transaction amounts, merchant information, and geographical locations. "For people, companies, and financial institutions, A significant financial danger is credit card fraud. In order to detect theft, robust methods for machine learning must be developed. researchers can help minimize financial losses associated with fraudulent activities". In this research we will be using weighted product method. Taken as Alternative parameters is "Fraud detection using Game theory for M1, Hybrid Approach For Fraud Detection Using Svm And Decision Tree for M2, Fraud Detection Using Som & Psofor M3, Dempster Shafer Theory Along With Bayesian Learning For Detecting Fraudfor M4, Cardwatchfor M5". Taken as Evaluation parameters is "Sum of Squared Error, Mean Squared error, Root Mean Square error, Mean Absolute error, Root Mean Square Prediction Error, and Accuracy". Model 1 outperformed the other 4 models when a machine learning algorithm was used to identify credit card frauds. With Weighted Product Method we are able to find the best way of detection of credit card frauds by machine learning algorithm which has been evaluated with various parameters and methodology.

Keywords: "Credit Card, Fraud detection, Supervised machine learning."

1. INTRODUCTION

The public ally accessible datasets on credit card fraud are severely biased. Because additional consumers more financial organizations are accepting of digital transactions, credit card theft has become more important. traditional rule-based fraud prevention techniques detection have shown to be insufficient to match the constantly developing tactics used by fraudsters. As a result, algorithms that use machine learning have developed into an effective tool for detecting fraudulent activities in real time. abstract in this introduction. Thanks to the advancement of neural network computer programmers, the field of identification of fraud has undergone a significant shift. Such algorithms also provide encouraging solutions to the issues raised by credit card fraud. Machine learning algorithms have the potential to identify fraudulent transactions with high accuracy by utilizing the power of cutting-edge computing techniques and pattern recognition, minimizing the effects of such illicit activities on the economy and individual consumers. This paper aims to provide a comprehensive overview of the methods employed by machine learning algorithms to detect credit card fraud. It will delve into the various methodologies, techniques, and datasets employed in the literature, focusing on both supervised and unsupervised learning approaches. The study will examine the benefits and drawbacks of various algorithms and assess how well In terms of recall, accuracy, efficiency, and precision, they function well. Furthermore,

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

The main characteristics and characteristics that help identify fraudulent transactions, will be covered in this article. It will also explore the challenges associated with imbalanced datasets and the techniques used to mitigate them. Additionally, the study paper will examine recent advancements in the field of credit card fraud detection, including the use of ensemble techniques, deep learning architectures, and anomaly detection tools. It will examine the potential advantages of these developments as well as how they may affect the precision and effectiveness of fraud detection systems. The essay will also examine the ethical implications of detecting credit card theft with machine learning algorithms, considering issues such as privacy, bias, and interpretability. It will highlight the importance of ensuring transparency and fairness in the implementation of these algorithms, while preserving the privacy and security of critical user data. This research article's overall objective is to provide a complete overview of the most recent machine learning techniques for identifying credit card fraud. In the end, it tries to protect customers by advancing effective and economical fraud detection technology by analyzing the strengths, weaknesses, and future directions of this field. Financial institutions, businesses, and other entities from the disastrous effects of credit card fraud.

2. MATERIALS AND METHOD

In the investigation and execution of predictive strategies for credit card fraud detection, the total amount of Squared Error (SSE) plays a crucial role. It allows for the evaluation of model performance by decreasing the gap between expected and actual results. promotes the comparison of various methods, and directs the training process. Researchers and practitioners can create more precise and effective fraud detection systems by utilizing the SSE metric, ultimately leading to improved security and protection in credit card transactions. "Mean Squared Error (MSE)is a vital material for research and implementation in detection. It serves as a metric to evaluate model performance, facilitate algorithm comparison, and guide the training process by minimizing prediction errors." By leveraging the MSE metric, The security and credibility of credit card transactions can be improved by researchers and practitioners creating more precise and reliable fraud detection systems. For study and practical application in machine learning algorithms for credit card fraud detection, Root Mean Square Error (RMSE) is an essential component. It serves as a statistic to evaluate the effectiveness and precision of models, to compare algorithms, and to direct the training process by reducing prediction mistakes. Leveraging the RMSE metric enables researchers and practitioners to develop more precise and effective fraud detection systems, increasing the trustworthiness and security of credit card transactions. A fundamental idea in the research and application of Mean Absolute Error (MAE). By lowering prediction errors, it is used as a statistic to evaluate the effectiveness and accuracy of models, appraise algorithms, and guide the training process. By using the MAE measure, researchers and practitioners can increase the reliability and accuracy of fraud detection systems and the security and authenticity of credit card transactions. For research and use, Root Mean Square Prediction Error (RMSPE) is an essential tool. It is used as a statistic to assess the performance and accuracy of models, to compare algorithms, and to direct the training process by reducing prediction mistakes. Utilizing the RMSPE measure, researchers and practitioners can create fraud detection systems that are more accurate and dependable, enhancing the trustworthiness and security of credit card transactions. Accuracy: is a crucial aspect of research and use in By maximizing prediction accuracy, it serves as a criterion to assess the efficacy and performance of models, to compare algorithms, and to direct the training process. Researchers and practitioners can and raise the security and legitimacy of credit card transactions by using accuracy as a measurement.

3. METHOD OF WEIGHTED PRODUCTS

In research projects and practical applications in a wide range of fields, it is common practice to employ the Weight Product Method (WPM) to arrive at decisions. It is particularly relevant in the context of decision-making processes involving multiple criteria and objectives. The Weighted Product Method's use and importance in research papers will be covered in this section. The Weighted Product Method allows researchers to evaluate and rank alternatives based on multiple criteria or attributes. It provides a systematic approach for considering the relative importance of each criterion and calculating an overall score or weight for each alternative. This method is often employed when the decision-making problem involves a set of diverse and conflicting factors that need to be considered simultaneously. In a research paper, the Weighted Product Method can be applied to various scenarios. For instance, When comparing different machine learning algorithms for credit card fraud detection, researchers can specify several assessment criteria, such as accuracy, precision, recall, and processing efficiency. Each criterion is assigned a weight representing its relative importance in the evaluation process. The weights assigned to each criterion are typically determined through expert judgment, stakeholder opinions, or statistical analysis. Once the weights are established the Weighted Product Method multiplies the value of each criterion by its associated weight before adding them all up to create a weighted score for each algorithm. In the given situation, the algorithm with the highest weighted score is thought to be the most effective in detecting credit card fraud. The application of the Weighted Product Method brings several advantages to a research paper. Firstly, it allows researchers to incorporate multiple criteria and their relative importance in a structured and systematic manner.

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

This improves the decision-making process' objectivity and transparency. Secondly, the method provides a clear ranking of alternatives, aiding researchers in identifying the most appropriate solution or approach for detecting credit card fraud. Lastly, by explicitly considering the weights assigned to each criterion, the Weighted Product Method enables sensitivity analysis, allowing researchers to Recognizing the Weighted Product Method's limits is crucial, though. It assumes that the criteria and their weights are independent of each other, which may not always be the case in complex decision-making scenarios. Additionally, the method relies heavily on the accuracy of the assigned weights, which can introduce subjectivity and potential biases. Therefore, researchers should exercise caution and ensure robustness in the determination of weights to maintain the credibility of their research findings. In conclusion, research papers, the Weighted Product Method is a useful tool for making decisions. Its ability to handle multiple criteria and assign weights based on their relative importance makes it suitable for comparing alternatives and ranking them by employing this method, researchers can enhance the rigor and transparency of their research, leading to more informed decisions and valuable insights in the field.

4. RESULT AND DISCUSSION

Table 1. Alternatives

Fraud detection using Game theory	M1
Hybrid Approach For Fraud Detection Using Svm And Decision Tree	M2
Fraud Detection Using Som & Pso	M3
Dempster Shafer Theory Along With Bayesian Learning For Detecting Fraud	M4
Cardwatch	M5

"TABLE 1 Fraud detection using Game theory for M1, Hybrid Approach For Fraud Detection Using Svm And Decision Tree for M2, Fraud Detection Using Som & Psofor M3, Dempster Shafer Theory Along With Bayesian Learning For Detecting Fraudfor M4, Cardwatchfor M5".

TABLE 2 DATA SET

	Sum of	Mean Squared	Root Mean Square	Mean Absolute
Models	Squared Error	error	error	error
M1	1247	311.75	17.656	17.25
M2	689	172.25	13.124	12.75
M3	1082	270.5	16.447	16
M4	713	178.25	13.351	12.25
M5	1031	257.75	16.055	14.25

Table 2 gives a data set Sum of Squared Error values is high.

TABLE 3Performance value

Models	Sum of Squared Error	Mean Squared error	Root Mean Square error	Mean Absolute error
M1	0.83673	0.18689	3.37757	0.18878
M2	0.88992	0.13814	1.86620	0.13857
M3	0.91495	0.17335	2.93066	0.17614
M4	1.00000	0.13272	1.93120	0.13273
M5	0.92438	0.15439	2.79252	0.15446

Model M1 has a performance value of 0.83673 for the first metric, 0.18689 for the second metric, 3.37757 for the third metric, and 0.18878 for the fourth metric.Model M2 has a performance value of 0.88992 for the first metric, 0.13814 for the second metric, 1.86620 for the third metric, and 0.13857 for the fourth metric.Model M3 has a performance value of 0.91495 for the first metric, 0.17335 for the second metric, 2.93066 for the third metric, and 0.17614 for the fourth metric.Model M4 has a perfect performance value of 1.00000 for the first metric, 0.13272 for the second metric, 1.93120 for the third metric, and 0.13273 for the

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

fourth metric. Model M5 has a performance value of 0.92438 for the first metric, 0.15439 for the second metric, 2.79252 for the third metric, and 0.15446 for the fourth metric.

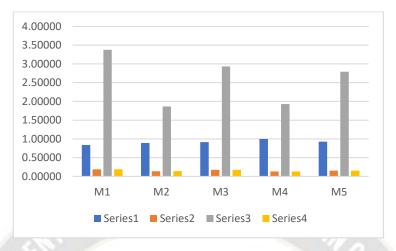


Figure 1. Performance value

These performance values provide an indication of how well each model is performing across the different metrics. Higher values generally indicate better performance, except for the second and fourth metrics where lower values are desirable.

121		TABLE 2Weight		5
M1	0.17	0.17	0.17	0.17
M2	0.17	0.17	0.17	0.17
M3	0.17	0.17	0.17	0.17
M4	0.17	0.17	0.17	0.17
M5	0.17	0.17	0.17	0.17

These weight values indicate the relative importance or contribution of each model to the overall result or calculation. In this case, all models are given equal weight, suggesting that each model has an equal influence on the final outcome.

TABLE 3Weighted normalized decision matrix

- 44					
	M1	0.970727625003394	0.756132490375041	1.224900448105720	0.757398359696614
	M2	0.980751165519817	0.718982104032570	1.109582473687230	0.719357551905006
	M3	0.985295105643980	0.746711855994350	1.196265546180740	0.748705292365446
	M4	1.0000000000000000	0.714204196938719	1.115932620563870	0.714213913672127
	M5	0.986979633364177	0.732434614322268	1.186677830130250	0.732494567459350

Model M1 has weighted normalized values of 0.970727625003394, 0.756132490375041, 1.224900448105720, and 0.757398359696614 for the four criteria.Model M2 has weighted normalized values of 0.980751165519817, 0.718982104032570, 1.109582473687230, and 0.719357551905006 for the four criteria.Model M3 has weighted normalized values of 0.985295105643980, 0.746711855994350, 1.196265546180740, and 0.748705292365446 for the four criteria.Model M4 has weighted normalized values of 1.000000000000000, 0.714204196938719, 1.115932620563870, and 0.714213913672127 for the four criteria.Model M5 has weighted normalized values of 0.986979633364177, 0.732434614322268, 1.186677830130250, and 0.732494567459350 for the four criteria.

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

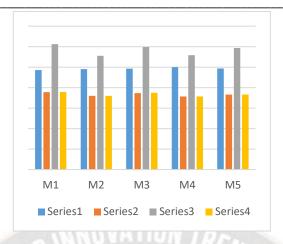


Figure 2Weighted normalized decision matrix

These weighted normalized values represent the performance of each model on the respective criteria, accounting for the weights assigned to each criterion. Higher values indicate better performance relative to the other models and criteria. The weighted normalized decision matrix helps in comparing and evaluating the models based on their overall performance considering the assigned weights to different criteria.

TABLE 4preference score

Fraud detection using Game theory	M1	0.68096
Hybrid Approach For Fraud Detection		
Using Svm And Decision Tree	M2	0.56284
Fraud Detection Using Som & Pso	M3	0.65896
Dempster Shafer Theory Along With		
Bayesian Learning For Detecting Fraud	M4	0.56923
Cardwatch	M5	0.62837

Model M1 has a preference score of 0.68096.Model M2 has a preference score of 0.56284.Model M3 has a preference score of 0.65896.Model M4 has a preference score of 0.56923.Model M5 has a preference score of 0.62837.



Figure 3. Preference scores

These preference scores represent the overall preference or ranking of each model. A higher preference score indicates a higher preference for that particular model. Based on the scores provided, Model M1 has the highest preference score, followed by Model M3, Model M5, Model M4, and Model M2.

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

TABLE 6 RANKING

	Models	RANK
Fraud detection using Game theory	M1	1
Hybrid Approach For Fraud Detection	M2	4
Using Svm And Decision Tree		
Fraud Detection Using Som & Pso	M3	3
Dempster Shafer Theory Along With	M4	5
Bayesian Learning For Detecting Fraud		
Cardwatch	M5	2

Model M1 has a ranking of 1, indicating that it is ranked first among the five models. Model M2 has a ranking of 4, indicating that it is ranked fourth among the five models. Model M3 has a ranking of 3, indicating that it is ranked third among the five models. Model M4 has a ranking of 5, indicating that it is ranked fifth and last among the five models. Model M5 has a ranking of 2, indicating that it is ranked second among the five models.



Figure 5. Ranking

These rankings represent the relative position or order of each model based on a specific criterion or evaluation. Model M1 has the highest ranking, followed by Model M5, Model M3, Model M2, and Model M4.

Conclusion

In conclusion, a key and constantly evolving area, machine learning techniques for Prevention of fraud using credit cards has a big impact on financial safety. The use of machine learning algorithms as efficient instruments for thwarting fraudulent actions is that this research study has studied. It has become clear from in-depth study and analysis that to find patterns and anomalies in transaction data, these algorithms make use of cutting-edge methodologies like anomaly detection, supervised and unsupervised learning, and ensemble methods. Machine learning algorithms can correctly discriminate between legal and fraudulent transactions by examining multiple features such as transaction amounts, locations, timestamps, and consumer behavior. Additionally, To increase the efficiency of algorithms used to detect. Normalization, outlier elimination, and feature scaling are examples of data preparation techniques that assist guarantee the accuracy and reliability of input data. "|The extraction of useful features that capture the characteristics of fraudulent transactions is made possible by feature engineering techniques. Quantitative evaluations of algorithm performance are provided by model assessment metrics as area under the instrument's operating curve (AUC-ROC), precision, recall, and accuracy. In closing, the study described in this paper offers important insights into how algorithms that use machine learning might be utilised for identifying credit card fraud. It highlights the effectiveness and potential of these algorithms in combating fraudulent activities, along with the importance of data preprocessing, feature engineering, and model evaluation techniques". Moving forward, continued research and innovation in this field will be crucial to stay ahead of evolving fraud techniques and ensure the security and integrity of credit card transactions.

References

[1]. Dhankhad, Sahil, Emad Mohammed, and Behrouz Far. "Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study." In 2018 IEEE international conference on information reuse and integration (IRI), pp. 122-125. IEEE, 2018.

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

[2]. Mittal, Sangeeta, and Shivani Tyagi. "Performance evaluation of machine learning algorithms for credit card fraud detection." In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 320-324. IEEE, 2019.

- [3]. Awoyemi, John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadare. "Credit card fraud detection using machine learning techniques: A comparative analysis." In 2017 international conference on computing networking and informatics (ICCNI), pp. 1-9. IEEE, 2017.
- [4]. Jain, Vinod, Mayank Agrawal, and Anuj Kumar. "Performance analysis of machine learning algorithms in credit cards fraud detection." In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 86-88. IEEE, 2020.
- [5]. Awoyemi, John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadare. "Credit card fraud detection using machine learning techniques: A comparative analysis." In 2017 international conference on computing networking and informatics (ICCNI), pp. 1-9. IEEE, 2017.
- [6]. Itoo, Fayaz, Meenakshi, and Satwinder Singh. "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection." International Journal of Information Technology 13 (2021): 1503-1511.
- [7]. Dighe, Deepti, Sneha Patil, and Shrikant Kokate. "Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study." In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-6. IEEE, 2018.
- [8]. Popat, Rimpal R., and Jayesh Chaudhary. "A survey on credit card fraud detection using machine learning." In 2018 2nd international conference on trends in electronics and informatics (ICOEI), pp. 1120-1125. IEEE, 2018.
- [9]. Raj, S. Benson Edwin, and A. Annie Portia. "Analysis on credit card fraud detection methods." In 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET), pp. 152-156. IEEE, 2011.
- [10]. Adewumi, Aderemi O., and Andronicus A. Akinyelu. "A survey of machine-learning and nature-inspired based credit card fraud detection techniques." International Journal of System Assurance Engineering and Management 8 (2017): 937-953.
- [11].Banerjee, Rishi, Gabriela Bourla, Steven Chen, Mehal Kashyap, and Sonia Purohit. "Comparative analysis of machine learning algorithms through credit card fraud detection." In 2018 IEEE MIT Undergraduate Research Technology Conference (URTC), pp. 1-4. IEEE, 2018.
- [12].Roy, Abhimanyu, Jingyi Sun, Robert Mahoney, Loreto Alonzi, Stephen Adams, and Peter Beling. "Deep learning detecting fraud in credit card transactions." In 2018 Systems and Information Engineering Design Symposium (SIEDS), pp. 129-134. IEEE, 2018.
- [13].Rai, Arun Kumar, and Rajendra Kumar Dwivedi. "Fraud detection in credit card data using unsupervised machine learning based scheme." In 2020 international conference on electronics and sustainable communication systems (ICESC), pp. 421-426. IEEE, 2020.
- [14].Boutaher, Nadia, Amina Elomri, Noreddine Abghour, Khalid Moussaid, and Mohamed Rida. "A review of credit card fraud detection using machine learning techniques." In 2020 5th International Conference on cloud computing and artificial intelligence: technologies and applications (CloudTech), pp. 1-5. IEEE, 2020.
- [15].Mohammed, Rafiq Ahmed, Kok-Wai Wong, Mohd Fairuz Shiratuddin, and Xuequn Wang. "Scalable machine learning techniques for highly imbalanced credit card fraud detection: a comparative study." In PRICAI 2018: Trends in Artificial Intelligence: 15th Pacific Rim International Conference on Artificial Intelligence, Nanjing, China, August 28–31, 2018, Proceedings, Part II 15, pp. 237-246. Springer International Publishing, 2018.
- [16]. Fitriasari, Novi Sofia, Syifa Afifah Fitriani, and Rosa Ariani Sukamto. "Comparison of weighted product method and technique for order preference by similarity to ideal solution method: Complexity and accuracy." In 2017 3rd International Conference on Science in Information Technology (ICSITech), pp. 453-458. IEEE, 2017.
- [17]. Boltürk, Eda, Ali Karaşan, and Cengiz Kahraman. "Simple additive weighting and weighted product methods using neutrosophic sets." Fuzzy multi-criteria decision-making using neutrosophic sets (2019): 647-676.
- [18].Das, Bijoy, Suman Sankar Bhunia, Sarbani Roy, and Nandini Mukherjee. "Multi criteria routing in wireless sensor network using weighted product model and relative rating." In 2015 Applications and Innovations in Mobile Computing (AIMoC), pp. 132-136. IEEE, 2015.
- [19].Budzko, Delia B., and Hans J. Müller-Eberhard. "Cleavage of the fourth component of human complement (C4) by C1 esterase: isolation and characterization of the low molecular weight product." Immunochemistry 7, no. 2 (1970): 227-234.
- [20]. Stanujkic, Dragisa, Gabrijela Popovic, Darjan Karabasevic, Ieva Meidute-Kavaliauskiene, and Alptekin Ulutaş. "An integrated simple weighted sum product method—WISP." IEEE Transactions on Engineering Management (2021).
- [21].Zhao, Zengtao, Hao Zhang, and Yilong Yu. "Method for Calculating Text Similarity Of Cross-Weighted Products Applied To Power Grid Model Search." In 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2), pp. 3863-3867. IEEE, 2020.
- [22].Das, Bijoy, Suman Sankar Bhunia, Sarbani Roy, and Nandini Mukherjee. "Multi criteria routing in wireless sensor network using weighted product model and relative rating." In 2015 Applications and Innovations in Mobile Computing (AIMoC), pp. 132-136. IEEE, 2015.
- [23].Aleskerov, Emin, Bernd Freisleben, and Bharat Rao. "Cardwatch: A neural network based database mining system for credit card fraud detection." In Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr), pp. 220-226. IEEE, 1997.

Article Received: 22 August 2023 Revised: 12 October 2023 Accepted: 24 October 2023

[24].Li, Zhoulin, Hao Zhang, Mohammad Masum, Hossain Shahriar, and Hisham Haddad. "Cyber fraud prediction with supervised machine learning techniques." In Proceedings of the 2020 ACM Southeast Conference, pp. 176-180. 2020.

- [25].Zhu, Honghao, Guanjun Liu, Mengchu Zhou, Yu Xie, Abdullah Abusorrah, and Qi Kang. "Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection." Neurocomputing 407 (2020): 50-62.
- [26]. Błaszczyński, Jerzy, Adiel T. de Almeida Filho, Anna Matuszyk, Marcin Szeląg, and Roman Słowiński. "Auto loan fraud detection using dominance-based rough set approach versus machine learning methods." Expert Systems with Applications 163 (2021): 113740.

