International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Review Article

A Review of Anomaly Identification in Finance Frauds using Machine Learning System

Sreenivasulu Gajula*

Principal Full-Stack Engineer

Received 26 Nov 2023, Accepted 05 Dec 2023, Available online 15 Dec 2023, **Vol.13, No.6 (Nov/Dec 2023)**

Abstract

The growing prevalence of digital financial payments has caused fraud in financial services to significantly increase globally. Artificial learning-based abnormality to identifying anomalies must be used because traditional fraud detection methods are not very adaptable to contemporary dishonest methods. This review investigates a variety of machine learning methodologies, such as deep learning, and the techniques used to detect fraud in banking, insurance, stock market processes, and digital payment transactions. The methods used include autonomous, freestanding, and semi-supervised learning. The study highlights challenges associated with imbalanced data distributions and adversarial attacks, which impact detection performance and interpretability. Furthermore, the study investigates current advances in the integration of transparent artificial intelligence with graph-based anomaly identification technologies to enhance the transparency and credibility of fraud detection systems. The investigation's constraints are reviewed to lead the construction of modern counterfeiting detection platforms that use numerous machine learning approaches for better accuracy, real-time processing, and privacy preservation. The findings provide insights into designing robust fraud detection systems aligned with banking institutions' requirements, ensuring enhanced financial security and compliance.

Keywords: *Anomaly Detection, Financial Fraud, Machine Learning, Fraud Detection, Credit Card*

Introduction

Financial statements serve as critical documents that encapsulate a company's financial performance, encompassing income, expenses, profits, loans, and managerial commentary. These statements, published quarterly and annually, provide transparency regarding business activities and allow stakeholders to evaluate the financial health and operational efficiency of an organization[1]. However, fraudulent manipulation of financial statements and transactions has emerged as a significant challenge, leading to substantial economic losses for governments, organizations, corporate entities, and individuals. Financial fraud undermines the integrity of financial institutions, eroding public trust and impacting the overall economy. It encompasses illicit activities that result in unauthorized financial gains through unethical or illegal means[2][3].

Anomaly detection contributes significantly to the detection of fraudulent activity by spotting anomalous patterns that diverge from typical transactional behavior[4].

*Corresponding author's ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.13.6.9

The identification of outliers and the detection of anomalies are frequently used indiscriminately, as they both focus on identifying deviations from expected behaviors[5][6]. Various techniques have been developed for anomaly detection, leveraging data mining and ML methodologies to uncover fraudulent financial activities. These anomalies, also referred to as discordant objects, exceptions, aberrations, or contaminants, are indicative of potential fraudulent behavior.

To safeguard financial systems, organizations invest significantly in advanced technology and safety precautions to guard against attacks from the inside and the outside[7][8]. Data-driven approaches[9], particularly those based on graph-based learning, have gained prominence in monitoring interactions and transactions within financial networks[10]. The relationships among entities in a network are analyzed by applying ML techniques to identify underlying irregularities that could signal fraudulent activities[11][12].

Traditional fraud detection models typically operate on structured attribute-value datasets derived from transactional records. These models categorise transactions as either legal or fraudulent using supervised and unsupervised learning approaches[13][14]. However, challenges arise in

detecting complex fraudulent behaviors such as money laundering, where transactions are inherently linked rather than independently distributed. The interdependencies in financial transactions necessitate advanced analytical models capable of handling linked data, which traditional methods often fail to address effectively[15].

ML financial methods for detecting fraud have become widely employed in a range of industries, including stock market fraudulent activities and fraudulent usage of credit cards[16], and other types of financial transaction anomalies. Recent studies have conducted comprehensive reviews on ML-driven fraud detection approaches, highlighting their effectiveness in mitigating fraudulent activities[17][18]. The evolution of ML-based techniques has significantly contributed to identifying and stopping financial fraud, providing a foundation for future research in this domain[19].

Structured of the paper

The paper is organized as following sections: Section II Methods for detecting anomalies in financial fraud Section III provide a ML approaches for financial fraud detection. Section IV Challenges, Limitations and future trends. Section V Literature Review, and Section VI concludes with future directions.

Anomaly Detection Techniques in Financial Fraud

An anomaly identification technology for banking activities is called Deception Surveillance. Deception Guard learns how a user's financial transactions typically behave using ML. Transactions are marked as questionable if they diverge beyond this typical pattern. Finding uncommon or abnormal data in a dataset is the primary goal of identifying anomalies and a crucial component of information mining. The ability to instinctively recognize intriguing and uncommon patterns in datasets makes recognizing anomalies fascinating. In statistical and ML, anomalous detection, also referred to as outlier identification, aberration being noticed, strangeness being noticed, and exception mining, has been extensively researched. When they may lead to crucial actions in a variety of pertinent areas, irregularities are relevant due to how they signal noteworthy but infrequent occurrences.

Anomaly Detection Techniques

The methods for supervised learning NN and DT are important yet uncommon occurrences that may lead to important decisions in a variety of different application areas. Identify fraud events with labeled data through extensive dataset requirements[20][21]. Self-Training and Variational Autoencoders as a technique enable semi-supervised learning systems to enhance their detection capability through the unification of small labeled data sets with unlimited unlabeled data[22]. The anomaly detection approach in Unsupervised learning employs Isolation Forest and Autoencoders as tools for finding fraudulent patterns without requiring supervised tag[23]s. These detection procedures work best for identifying new fraudulent activities shown in Figure 1.

Supervised Anomaly: Supervised identification of anomalies techniques are predicated on the utilisation of a data set consisting of annotated cases that fall into either the normal or anomalous class [24][25]. The majority of methods in the latter group provide a prediction model for the normal and abnormal classes, which can then be used to classify newly discovered data. As was briefly mentioned before, a major problem with autonomous detecting anomalies is that the atypical class is often less common than the regular class[26].

Semi-supervised Anomaly: Anomaly detection methods that rely on semi-supervised learning presume that all instances in the dataset have been marked to belong to a standard class. They are thus more relevant[27]. In contrast with unsupervised anomalies of anomalies, a framework is only built for the standard category and not the abnormal class. To find unusual occurrences, the test set of data is then contrasted with the model[28].

Unsupervised Anomaly: Naturally all three groups, uncontrolled recognition without supervision is the most universally useful as the methods don't need any labels in the information set. In order to avoid larger instances of false alarms than anticipated, uncontrolled algorithms implicitly assume that abnormal occurrences are much less common than ordinary occurrences in the under scrutiny set of the information under consideration[29][30]. An unlabeled subsection of the training set of data is often used to apply semi-supervised techniques to an uncontrolled identification of anomaly issues.

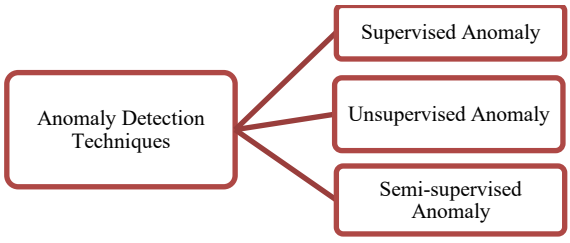

Fig.1 Anomaly Detection Techniques

Types of Anomalies

There are three types of abnormalities individual deviations, which are irregular data points contextual anomalies, which are normal in one context but aberrant in a different one; and aggregate anomalies, which are a collection of connected outliers indicating fraud). There are some of the anomaly types are explained below in Figure 2.

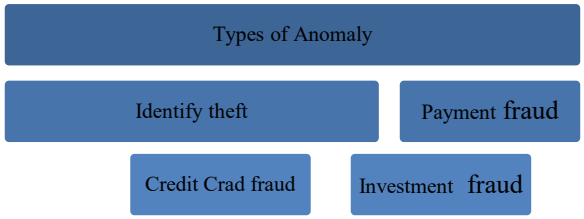

Fig.2 Types of Anomaly

Identity Theft: The theft of identity is the unlawful acquisition and use of private data, such as banking account details or a social security number, with the goal of committing fraud. More complex methods of stealing someone's identity have also been made possible by developments in technology.

Payment Fraud: The practices that target money transactions, such as credit card and cheque fraud, are included in fraud involving payments[31]. FIs should use diligence procedures while dealing with transactions and keep an eye out for anomalies in payment trends.

Credit Card Fraud: The fraudulent use of credit cards is the most ancient and common type of fraud, along with identity theft[32]. It is the unauthorised use of a person's debit or credit card to make purchases or withdraw cash.

Investment Fraud: The numerous strategies covered in this article are used in investment scams and frauds. Since fraudsters will go to considerable measures to make any web pages[33], papers, or information mentioned seem as authentic as achievable, many are going to be simpler to identify than others.

Machine Learning Approaches for Financial Fraud Detection

There are numerous algorithms available for detecting fraud. However, because it all relies on what information you presently have, there isn't a single best ML technique for fraud detection. Figure 3 displays a list of some of the most well-known techniques; nevertheless, this is by no means an exhaustive list.

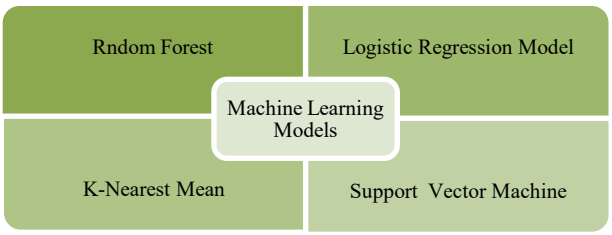

Fig.3 Machine learning models

Logistic Regression (LR) Model

A popular statistical framework for applications involving classifications that are binary is LR[34]. It is a classification technique, not a regressive method, as the title suggests. It calculates the likelihood that a certain input is a member of a specified class. The LR model maps expected values to possibilities using the logistic function. The logistic function's outcome involves 0 and 1. LR divides inputs into two groups by establishing a threshold, often 0.5. using clinical data to determine whether a patient has a certain condition (such as diabetes or heart disease). Estimating the likelihood that a borrower would miss payments on a loan. using demographic and behavioral data to forecast a consumer's chances of making a buying decision

Support Vector Machines Model (SVM)

The two-class classification challenges were first addressed by proposing Support Vector Machines (SVM)[35]. The SVM reduces its generalisation error by dealing with the idea of structural risk minimisation. A best-fitting separating hyperplane (OSH) between sets of data is sought after. Optimising the margin between training sample classes is the primary objective. The promising extension of support vector machine (SVM) to tackle regression issues is support vector regression (SVR). Many applications and academic disciplines have found success with this method.

Decision Tree (DT) Model

The Testing and regression tasks benefit from the adaptable ML method known as decision trees. Each node in their decision structures represents a decision alongside its potential consequences that form a tree arrangement. The features in the model appear as nodes within the decision tree, while decision rules exist as connecting branches between nodes that lead to outcome leaves. The data splitting process at nodes depends on the feature which produces the most uniform subsets through an evaluation method (such as Gini impurity or information gain). Random forests comprise many decision trees that use the "bagging" approach for their training. The produced result of a random forest ensemble comes from averaging regression outputs and implementing majority voting for classification[36]. Forecasting the course of therapy and the outcomes for patients. Identification of fraud and risk control. Systems for client grouping and endorsement.

Random Forest Model

The introduction of ensemble decision-tree-based algorithms solved the overfitting issue of decision trees while random forest stands as a leading accurate and practical choice. Random forest classifiers construct

several decision trees which merge their predictions through voting. Randomization emerges from both bagging and feature random sub-setting procedures. Through bootstrapping methods different data becomes available for tree creation while feature subset selection performs two-way randomization leading to consolidated weak learner models.

K-Nearest Mean (KNN) Model

A financial institution organized equivalent transactions using K-means clustering methods. Further evaluation occurred for all transactions that did not belong to any cluster grouping. This method uncovered new fraud patterns which enhanced the institution's fraud prevention capabilities during the process of identifying trading fraud activities. Unsupervised anomaly detection methods identified transactions with abnormal behavior patterns through trading behavior analysis. The firm succeeded in uncovering insider trading infringements that routine inspection systems had overlooked. Detecting fraudulent insurance claims. The insurance organization used association rule learning to inspect their claims data through analysis. The analysis revealed unexpected patterns linking unconnected claims which thus made it possible to discover cooperative fraud activities

The Advantages of Machine Learning for Fraud Management

There are some advantages of ML for fraud are explained below[36]:

Faster and efficient detection: Machines are able to cut and paste enormous amounts of data given that they can process large datasets far more quickly than humans. That suggests More efficient and quick identifying objects The system is able to identify questionable trends and behaviors that individual employees would have missed for months.

Reduced manual review time: Similar to this, it's possible to substantially cut the amount of time on spend browsing over material by having computers review all of the evidence points for with that.

Larger datasets improve predictions: The greater amount of information you give an ML vehicle's engine, the more proficient it becomes. As a result, whereas huge amounts of data might often make it hard for humans to see patterns, an AI-driven system has exactly the opposite problem.

Cost-effective remedy: Instead of integrating more Risks agents, you just need one machine-learning system to handle all the data that you throw at it, no matter how much of information you have. This is ideal for businesses who see seasonal variations in

Challenges, Limitations And Future Directions In Financial Fraud Detection

Numerous advanced difficulties arise during the application of ML technology to detect financial fraud. The manifestation of fraud incidents remains lower than financial operations due to dataset imbalance which impedes model performance. The mechanisms used in fraud operations keep changing because criminals constantly advance their schemes to avoid detection protocols. Such adversarial attacks operate as an additional sixth method to modify ML models which enable attackers to escape identification systems. Multiple data types including transactions and user behaviors require refined integration methods because of their complex integration process. Synthetic data combines with obfuscation methods which fraudsters use to dodge detection systems among other forms of deception. False positive findings that break legal or ethical standards present a severe requirement since they generate financial losses for customers and lead to poor service satisfaction rates. The challenge is described below and also mentioned in Figure 4.

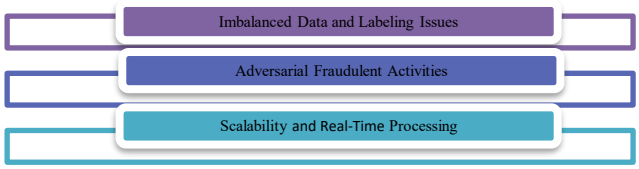

Fig.4 Challenges of Financial Fraud

Imbalanced Data and Labeling Issues

The newest statistics may change in minutes or seconds. Thus, standard categorisation may fail. Supervised education fails when the dataset has many regional inequalities, variable information, high complexity, and problem volume.

The growth of online transactions has skyrocketed in recent times and credit cards represent a significant portion of total online spending. An increasing number of people select credit cards to shop and execute e-commerce activities and educational transactions alongside e-wallet payments. Because banks and other involved stakeholders place high importance on fraud detection technology, they prioritize its development and maintenance. A wide range of fraudulent transactions exists. Online and Offline transactions represent their distribution. The research focuses on online transactions for explaining the ML solutions as an approach to managing them[37].

Adversarial Fraudulent Activities

A static paradigm that serves as a filter for these fraudulent and legitimate activities is the standard paradigm for detecting fraud. However, reality depicts a very tense relationship between criminals and financial institutions, especially considering the high cost of credit card theft and the ease with which stolen

credit card data can be retrieved from the dark web. In an effort to maximize stolen funds, fraudsters are always changing their tactics and trying to get past the fraud recognition algorithms. Credit card issuers' data scientists invest a lot of time and resources in thwarting fraudsters' attempts to learn the classifier and undermine its efficacy.

Scalability and Real-Time Processing

The analysis of data as it happens remains vital in finance sector applications because transaction surveillance requires instant data evaluation to track scams. The processing starts by collecting data which requires preprocessing. Different types of transaction data originate from point-of-sale mechanisms, online payments, mobile payment applications and bank wire transfers. The different sources deliver important results which enable the detection of financial fraud. Point-of-sale systems obtain retail transaction information simultaneously with online platform data collection for e-commerce recordings. Mobile payment systems enrich security by providing both user device information along with transaction location data to enrich authentication and detection capabilities for transaction data.

Future Trends in ML for Fraud Prevention

ML is developing quickly, with new developments in technology and trends influencing how prevention of fraud is done in the future. The subsequent sections emphasize important developments, such as the adoption of predictive as well as prescriptive analytics, the advancement of algorithms, the integration of other developing technology, and the growing emphasis on immediate data analysis. The following explains some possible paths in the future:

Explainable AI (XAI): Explore the complex areas of study and advancement related to Explainable AI (XAI). Deciphering the complexities of these approaches seeks to shed light on the opaque character of intricate models, opening the door for an explosion in openness that fosters confidence amongst law enforcement and investors alike.

Continuous Learning Models: The creation of models starts as a dance with shifting fraud patterns. The system's real-time performance optimization occurs through dynamic online learning approaches orchestrated for continuous learning, which directs systems to serenely adjust when faced with fraud dynamics transformations.

Hybrid Models and Ensemble Approaches: Explore the unexplored realms of model fusion using the alchemy of hybrid techniques and ensemble techniques. By combining the distinct brilliance of many models, an exquisite tapestry of fraud detection skill emerges, improving resistance and effectiveness.

Blockchain Technology: The secretive understand sound of blockchain technology while exploring its implementation to make data security systems more resilient during financial transactions. Smart contracts deployed on blockchain platforms serve as a potential peak solution within digital soundscape that builds fraud-resistant financial security system[38].

Collaboration and Benchmarking: Cultivate a cooperative environment between industry and educational institutions, planting the seeds for benchmarking measurements and datasets. The development of increasingly efficient fraud detection models is driven towards a harmonic conclusion by this musical standardization, which regulates fair assessments.

Literature Review

This section offers a thorough analysis of the research on machine learning-based anomaly detection in financial fraud.

Ali et al., (2022b) describes the most popular ML algorithms for fraud detection, types of fraud, and evaluation criteria. Based on the articles that were analysed, it appears that credit card fraud is the most prevalent type of fraud that ML approaches try to detect. Among the most well-known ML techniques utilised for this task are ANNs and support vector machines (SVMs). At last, the article lays out the key points, limitations, and problems with financial fraud detection, before proposing some avenues for further study. The goal of financial fraud is to get monetary gains using deceitful and unlawful means. The insurance, banking, tax, and corporate spheres are only a few examples of the many possible forums for financial fraud[17].

Turaba et al. (2022) provide the results of many tests that pertain to the identification of credit card counterfeits. The following is a comparison of three different algorithms: AdaBoost, CNN with GRU and Regular Neural Network. To rectify the dataset's imbalance, we employ an oversampling technique called Synthetic Minority Oversampling Technique (SMOTE). Convolution Neural Networks outperform all others in terms of accuracy, precision, recall, and area under the curve (AUC-ROC) [39].

Silva et al., (2021) have suggested a system that employs adversarial autoencoders and machine learning approaches to objectively categorise transactions as regular, local, or global anomaly. Supervised learning algorithms are fed features from the autoencoder-generated latent vectors as part of the integration. Various forms of latent vector spaces were investigated in the experiments, with respect to their dimensions and the clusters produced by a previous Gaussian mixture. The findings demonstrate that certain classifiers are able to effectively include latent variables, leading to comparable or even superior performance when all original attributes are used[40].

Abad-Segura and González-Zamar (2020) findings include information about the research efforts of the countries, organisations, writers, and institutions that support this area of study. An upward tendency, most pronounced in the recent ten years, is shown by the data. Economics, finance, and the social sciences make up the bulk of the body of knowledge. Among Indian Institute of Management Rohtak faculty, Khare has penned the most articles. The University of Oxford in the United Kingdom is the most prolific affiliate. As far as scholarly articles and international partnerships are concerned, the United States ranks first. Furthermore, "financial transaction tax," "financial management," "financial service," "banking," "blockchain," "financial market" and "decision making," are the most often used keywords in publications. Publications on a global scale have been on the rise in recent years, lending credence to the idea that studies of financial transactions are becoming increasingly popular[41].

Boutaher et al. (2020)article aims to lay out the fundamentals of fraud detection, go over the present systems for detecting fraud, talk about the challenges and concerns with fraud in the banking sector, and then detail the machine learning-based solutions that are available. Healthcare, finance, manufacturing, transportation, and e-commerce are just a few of the vital industries that big data technologies are impacting. The advent of digital services and e-commerce has caused significant shifts in the banking and financial sectors, making their continued relevance paramount[42].

Minastireanu and Mesnita (2019) Identifying and evaluating algorithms used for fraud detection according to predetermined standards is the goal of this presentation. To go through the research on fraud detection, we employed a systematic quantitative literature review approach. A hierarchical classification system is based on the characteristics of the most often cited machine learning algorithms in academic publications. Therefore, it uncovers the most effective approaches for detecting fraud by merging coverage, costs, and accuracy in a revolutionary way[43].

Table I presents a systematic summary of current studies on anomaly detection in financial fraud using ML. It emphasises the study's focus area, major findings, problems, and future research directions.

Table 1 Summary of Anomaly Detection in Financial Frauds Using Machine Learning approaches

Reference	Focus Area	Key Findings	Challenges	Future Work & Limitations
Ali et al. (2022b)	ML techniques in financial fraud detection	SVM and ANN are commonly used; credit card fraud is the most targeted	Identified issues in existing fraud detection methods	Suggests further research on improving fraud detection models and addressing identified gaps
Turaba et al. (2022)	Credit card counterfeit detection	CNN with GRU outperforms others; SMOTE improves performance on imbalanced datasets	Data imbalance and model comparison	More robust models and handling of imbalance with advanced techniques
Silva et al. (2021)	Anomaly detection using adversarial autoencoders	Latent features from autoencoders improve or match traditional features in classification tasks	Determining optimal latent space and classifier compatibility	Further studies on feature space optimization and classifier tuning
Abad-Segura & González-Zamar (2020)	Global research trends in financial transaction fraud	U.S. leads research; focus on keywords like “blockchain”, “banking”, and “financial market”	Limited research in some regions and disciplines	Calls for broader collaboration and interdisciplinary research
Boutaher et al. (2020)	ML in banking sector fraud detection	Defines fraud detection aspects and solutions using ML in Big Data environments	Rapid digital evolution and complex e-commerce transactions	Emphasis on ML model enhancement and adaptability to digital transformation
Minastireanu & Mesnita (2019)	Algorithm comparison for fraud detection	Developed typology using accuracy, coverage, and cost criteria	Difficulty in algorithm selection based on varied evaluation metrics	Suggests combining selection criteria for better fraud detection method applicability

Conclusion and Future Work

The application of ML techniques enables financial institutions to successfully detect anomalous transactions for protecting themselves against risks through successful results. The three main types of machine learning—unsupervised learning, graph-based learning and supervised learning—are all helpful in identifying various forms of financial fraud. Unbalanced dataset issues, changes in fraudulent techniques, and the need for interpretable models while managing data privacy concerns make it challenging to develop reliable fraud detection systems. While LR and DT, two common ML models, provide basic achievement, deep learning, when used in conjunction with GNNs performs better when applied to complicated patterns. fraud patterns. The continuous evolution of fraud detection strategies highlights the need for adaptive and scalable models to combat emerging threats in the financial sector.

Research in the future should focus on developing more efficient and adaptable fraud detection systems that combine explainable AI methods with real-time anomaly detection. The use of hybrid models combining deep learning and traditional ML approaches can further improve detection accuracy. Additionally, addressing data privacy challenges through federated learning and blockchain-based fraud

detection could enhance security while maintaining confidentiality. Moreover, the development of cost-sensitive models that minimize false positives without compromising fraud detection rates is crucial. Future studies should also explore automated feature engineering techniques and self-learning systems that can adapt to new fraud patterns with minimal human intervention. Finally, financial institutions and regulators can collaborate to create industry-wide fraud detection frameworks.

References

[1] M. N. Ashtiani and B. Raahemi, "Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review," 2022. doi: 10.1109/ACCESS.2021.3096799.

[2] M. Alamri and M. Ykhlef, "Survey of Credit Card Anomaly and Fraud Detection Using Sampling Techniques," 2022. doi: 10.3390/electronics11234003.

[3] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," 2021. doi: 10.1016/j.cosrev.2021.100402.

[4] A. Beteto et al., "Anomaly and cyber fraud detection in pipelines and supply chains for liquid fuels," Environ. Syst. Decis., 2022, doi: 10.1007/s10669-022-09843-5.

[5] A. and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, 2021, doi: https://doi.org/10.14741/ijcet/v.11.6.11.

[6] A. Balasubramanian, "Building Secure Cybersecurity Infrastructure: Integrating Ai And Hardware For Real-Time Threat Analysis," Int. J. Core Eng. Manag., vol. 6, no. 07, pp. 263–271, 2020.

[7] T. Ashfaq et al., "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism," Sensors, 2022, doi: 10.3390/s22197162.

[8] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," ESP J. Eng. Technol. Adv., vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

[9] S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," Int. J. Curr. Eng. Technol., vol. 12, no. 6, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.11.

[10] T. Pourhabibi, K. L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," Decis. Support Syst., 2020, doi: 10.1016/j.dss.2020.113303.

[11] S. Chatterjee, "Mitigating Supply Chain Malware Risks in Operational Technology : Challenges and Solutions for the Oil and Gas Industry," vol. 12, no. 2, pp. 1–12, 2021.

[12] M. J. Shayegan, H. R. Sabor, M. Uddin, and C. L. Chen, "A Collective Anomaly Detection Technique to Detect Crypto Wallet Frauds on Bitcoin Network," Symmetry (Basel)., 2022, doi: 10.3390/sym14020328.

[13] M. Shah and A. Goginen, "Distributed Query Optimization forPetabyte-Scale Databases," Int. J. Recent Innov. Trends Comput. Commun., vol. 10, no. 10, 2022.

[14] D. Huang, D. Mu, L. Yang, and X. Cai, "CoDetect: Financial Fraud Detection with Anomaly Feature Detection," IEEE Access, 2018, doi: 10.1109/ACCESS.2018.2816564.

[15] A. Westerski, R. Kanagasabai, E. Shaham, A. Narayanan, J. Wong, and M. Singh, "Explainable anomaly detection for procurement fraud identification—lessons from practical deployments," Int. Trans. Oper. Res., 2021, doi: 10.1111/itor.12968.

[16] G. Moschini, R. Houssou, J. Bovay, and S. Robert-Nicoud, "Anomaly and Fraud Detection in Credit Card Transactions Using the ARIMA Model †," Eng. Proc., 2021, doi: 10.3390/engproc2021005056.

[17] A. Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," 2022. doi: 10.3390/app12199637.

[18] S. S. S. Neeli, "Key Challenges and Strategies in Managing Databases for Data Science and Machine Learning," Int. J. Lead. Res. Publ., vol. 2, no. 3, p. 9, 2021.

[19] S. Tyagi, T. Jindal, S. H. Krishna, S. M. Hassen, S. K. Shukla, and C. Kaur, "Comparative Analysis of Artificial Intelligence and its Powered Technologies Applications in the Finance Sector," in 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022, pp. 260–264. doi: 10.1109/IC3I56241.2022.10073077.

[20] R. Tarafdar and Y. Han, "Finding Majority for Integer Elements," J. Comput. Sci. Coll., vol. 33, no. 5, pp. 187–191, 2018.

[21] V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," 2022

[22] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based Iot Network.," J. Crit. Rev., 2019.

[23] V. Kolluri, "An In-Depth Exploration of Unveiling Vulnerabilities: Exploring Risks in AI Models and Algorithms," Int. J. Res. Anal. Rev., vol. 1, no. 3, pp. 910–913, 2014.

[24] Á. G. Faura, D. Štepec, M. Cankar, and M. Humar, "Application of unsupervised anomaly detection techniques to moisture content data fromwood constructions," Forests, 2021, doi: 10.3390/f12020194.

[25] A. V. Hazarika and Anju, "Extreme Gradient Boosting using Squared Logistics Loss function," Int. J. Sci. Dev. Res., vol. 2, no. 8, pp. 54–61, 2017.

[26] N. Görnitz, M. Kloft, K. Rieck, and U. Brefeld, "Toward supervised anomaly detection," J. Artif. Intell. Res., 2013, doi: 10.1613/jair.3623.

[27] V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization Ai for Cybersecurity Incident Investigations," Int. J. Res. Anal. Rev. (IJRAR, vol. 3, no. 3, 2016.

[28] L. Ruff et al., "Deep Semi-Supervised Anomaly Detection," in 8th International Conference on Learning Representations, ICLR 2020, 2020.

[29] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," IEEE Access, 2019, doi: 10.1109/ACCESS.2019.2953095.

[30] A. Polleri, R. Kumar, M. Bron, and G. Chen, "Identifying a classification hierarchy using a trained machine learning pipeline," 2022

[31] M.-H. Yang, J.-N. Luo, M. Vijayalakshmi, and S. M. Shalinie, "Contactless Credit Cards Payment Fraud Protection by Ambient Authentication," Sensors, vol. 22, no. 5, p. 1989, Mar. 2022, doi: 10.3390/s22051989.

[32] E. Ileberi, Y. Sun, and Z. Wang, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3134330.

[33] M. Lokanan, "The determinants of investment fraud: A machine learning and artificial intelligence approach," Front. Big Data, vol. 5, Oct. 2022, doi: 10.3389/fdata.2022.961039.

[34] S. Mousa, G. Ramkumar, A. J. Mohamma, B. Othman, M. S. Narayana, and B. Pant, "Financial Market Sentiment

Prediction Technology and Application Based on Machine Learning Model," in 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2022, 2022. doi: 10.1109/ICACITE53722.2022.9823563.

[35] M. Sabzekar and S. M. H. Hasheminejad, "Robust regression using support vector regressions," Chaos, Solitons & Fractals, vol. 144, Mar. 2021, doi: 10.1016/j.chaos.2021.110738.

[36] S. U. Rabade, "Use of Machine Learning in Financial Fraud Detection: A Review," Int. J. Adv. Res. Sci. Commun. Technol., pp. 38–44, Nov. 2022, doi: 10.48175/IJARSCT-7595.

[37] M. K. R. Mallidi and Y. Zagabathuni, "Analysis of Credit Card Fraud detection using Machine Learning models on balanced and imbalanced datasets," Int. J. Emerg. Trends Eng. Res., vol. 9, no. 7, pp. 846–852, Jul. 2021, doi: 10.30534/ijeter/2021/02972021.

[38] S. Pandya, "Innovative blockchain solutions for enhanced security and verifiability of academic credentials," Int. J. Sci. Res. Arch., vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.

[39] M. Y. Turaba, M. Hasan, N. I. Khan, and H. A. Rahman, "Fraud Detection During Financial Transactions using Machine Learning and Deep Learning Techniques," in Proceedings of the 2022 IEEE International Conference on Communications, Computing, Cybersecurity and Informatics, CCCI 2022, 2022. doi: 10.1109/CCCI55352.2022.9926503.

[40] J. C. S. Silva, D. Macedo, C. Zanchettin, A. L. I. Oliveira, and A. T. de Almeida Filho, "Multi-Class Mobile Money Service Financial Fraud Detection by Integrating Supervised Learning with Adversarial Autoencoders," in 2021 International Joint Conference on Neural Networks (IJCNN), IEEE, Jul. 2021, pp. 1–7. doi: 10.1109/IJCNN52387.2021.9533313.

[41] E. Abad-Segura and M.-D. González-Zama, "Global Research Trends in Financial Transactions," Mathematics, vol. 8, no. 4, p. 614, Apr. 2020, doi: 10.3390/math8040614.

[42] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A Review of Credit Card Fraud Detection Using Machine Learning Techniques," in Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020, 2020. doi: 10.1109/CloudTech49835.2020.9365916.

[43] E. A. Minastireanu and G. Mesnita, "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," Inform. Econ., vol. 23, no. 1/2019, pp. 5–16, Mar. 2019, doi: 10.12948/issn14531305/23.1.2019.01.