A SYSTEMATIC REVIEW OF APPLICATIONS IN FRAUD DETECTION

Hashim Jameel Shareef Jarrar

Department of Cybersecurity, College of Information Technology, Middle East University, Amman, Jordan

ABSTRACT

The following systematic review aims to investigate the applications of data science techniques for fraud detection (FD), especially Machine Learning (ML),Deep Learning (DL), and the combination of both techniques in different domains, including credit card fraud and cyber (online) fraud. The increasing sophistication of fraudulent activities necessitates advanced detection methods, as traditional rule-based techniques often fall short. The review involves articles from 2022 to 2024, establishing various algorithms and techniques' efficiency. Some of the research findings show that the most frequently used FD algorithms are supervised ML algorithms like logistic regression, decision trees, and random forests, which have high accuracy. Also, DL techniques especially Long Short-Term Memory (LSTM) networks and convolutional neural networks (CNNs), have been reported to provide better results, especially in real-world problems, including e-commerce and online web-based FD. Some of the new trends that are increasingly being incorporated to improve FD capabilities are the hybrid models that integrate ML and DL methods. However, there are still some limitations associated with the use of ML for FD, such as class imbalance, interpretability of the trained model, and the evolving nature of fraud tactics. The review discusses the current trends, including real-time detection and the use of AI in FD systems; the review also provides further research directions for overcoming the challenges and improving the performance of FD systems. Overall, this review contributes to the growing body of knowledge in FD and emphasizes the importance of continuous innovation in data science applications.

KEYWORDS

Data Science; Machine Learning; Deep Learning; Fraud Detection; Cyber Fraud

1. INTRODUCTION

Fraud detection (FD) has become a critical issue in various industries, including finance, e-commerce, and cybercrimes, due to the increasing prevalence of fraudulent activities and the associated financial and reputational losses(Al-Hashedi & Magalingam, 2021). Traditional rule-based and anomaly detection techniques have proven ineffective in addressing modern fraud schemes' complexity and sophistication(Benedek & Nagy, 2023). However, the rapid advancements in data science, particularly in the fields of machine learning (ML), deep learning (DL), and artificial intelligence (AI) have revolutionized the way FD is approached. Data science techniques offer powerful tools for analyzing large volumes of data, identifying patterns, and detecting anomalies that may indicate fraudulent behavior. These techniques have been widely applied in various FD domains, such as credit card fraud and cyber (online) fraud (Abed & Fernando, 2023; Patel, 2023). The application of data science in FD has gained significant attention in recent years, with numerous studies exploring the effectiveness of different algorithms and techniques.

According to the Nilson Report, global CCF losses have steadily increased, reaching $28.65 billion in 2021. This represents a 10% increase from 2020 (Sinčák, 2023). The shift towards online and card-not-present (CNP) transactions has increased the risk of CCF, as it is more difficult to verify the cardholder's authenticity(Abed & Fernando, 2023). In Europe, CCF fell to its lowest level (0.028%) in 2021, driven by the implementation of robust customer authentication measures(Fatih, 2023). However, the UK continues to have the highest fraudster rates in Europe, with over £1.2 billion stolen via authorized and unauthorized activities in 2022(Saghir & Kafteranis, 2022).Globally, businesses in e-commerce, small businesses, and high-risk industries are particularly vulnerable to CCF. CCF includes stolen/lost cards, CNP fraud, account takeover, application fraud, skimming, and phishing/vishing scams. Ongoing vigilance and adopting advanced data science techniques are crucial to combat the evolving nature of CCF worldwide(Nicolini & Leonelli, 2021).

DOI: 10.5121/ijnsa.2025.17403

Furthermore, insurance fraud is also a growing global problem, with over 60% of surveyed insurers reporting a significant increase in fraud incidents over the past two years(Saddi et al., 2024). The financial impact is staggering, with healthcare fraud alone costing an estimated $105 billion annually in the US(Ashley Kilroy, 2024). Common insurance fraud schemes include false injuries, non-disclosure of relevant information, staged accidents, and fraudulent billing. Emerging trends indicate increased data theft, collusion between third parties, and mis-selling insurance products. Fraudsters are also taking advantage of the shift towards digitalization, tampering with electronic claims evidence. To combat this, insurers invest in advanced analytics and anti-fraud technologies like predictive modeling and link analysis(O'Brien, 2021). However, most insurers plan to maintain the same level of investment in fraud risk management, raising concerns about the effectiveness of current controls. Ongoing vigilance and collaboration between insurers, regulators, and law enforcement are crucial to stay ahead of evolving fraud tactics worldwide(Nalluri et al., 2023).

In 2023, the Federal Trade Commission received over one million reports of identity theft, with CCF being the most common type. Identity theft reports declined from 2022 but remained well above pre-pandemic levels. Fraudsters increasingly use sophisticated techniques like synthetic identity theft, which leverages AI to create fake identities. This type of fraud is estimated to cost lenders nearly $3 billion annually(Mitchell, 2023). Cybercriminals also target specific personal data in data breaches, leading to a surge in breaches despite a decliningnumber of affected individuals.CCF remains a significant issue, with lost or stolen cards accounting for most ATM and point-of-sale fraud(Berg & Hansen, 2020; Btoush et al., 2023). Ongoing vigilance and advanced FD technologies are crucial to combat these evolving threats.

This systematic review aims to comprehensively analyze the current research on data science applications in different FDs. By integrating the findings from relevant studies published between 2022 and 2024, this review seeks to identify the most effective techniques, highlight emerging trends, and uncover research gaps that warrant further investigation.

1. RESEARCH METHODOLOGY

A thorough analysis of this systematic review's working and reporting processes adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria statement(Page et al., 2021). Furthermore, no formal ethical review or informed consent was required because this was a review of already published studies.

2.1. Searching Strategy

We developed a search strategy for this systematic research to identify relevant literature. The search strategy involved querying multiple electronic databases and web search engines, including Scopus, ACM Digital Library, Web of Science, ScienceDirect, IEEE Xplore, Google Scholar, Semantic Scholar, and JSTOR for relevant articles published between January 2020 and May 2024. The search terms used were: ("data science" OR "machine learning" OR "deep learning") AND ("fraud detection" OR "fraud prevention" OR "anomaly detection" OR "credit card fraud" OR "online fraud" OR "web-based fraud" OR "cyber fraud").

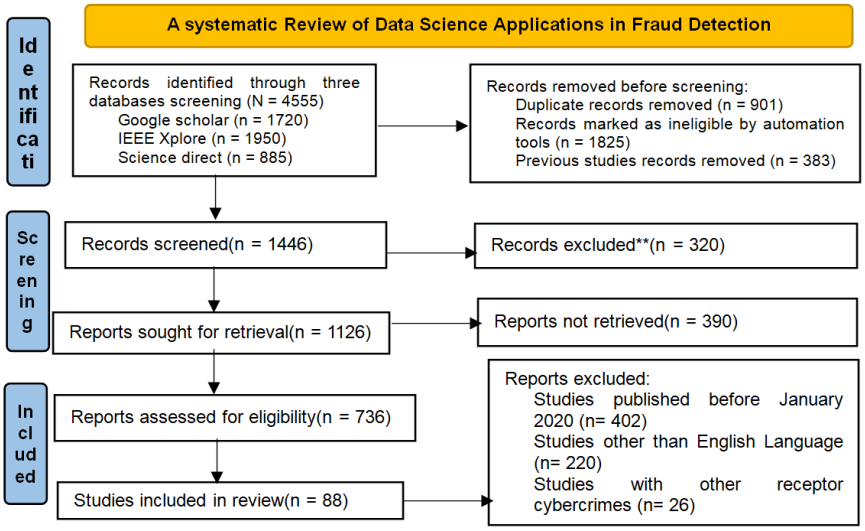

Figure 1. PRISMA flow diagram for the systematic review of data Science applications in fraud detection.

2.2. Inclusion Criteria

- Articles published in peer-reviewed journals or conference proceedings.
- Articles focusing on the application of data science techniques in FD.
- Articles focusing on only CCF, online fraud, and cyber fraud.
- Articles published between 2022-2024.
- Articles published in English.

2.3. Exclusion Criteria

- Articles published before January 2022 or after June 2024.
- Articles not accessible in full-text format.
- Articles not relevant to the scope of the review.

2.4. Data Collection and Extraction

The initial search yielded 4,555 articles. After removing duplicates and applying the inclusion and exclusion criteria, 736 articles were selected for full-text screening. Of these, 88 articles were deemed eligible for inclusion in the review.The data extraction process involved recording the following information for each included article: author names, publication year, journal or conference name, FD domain, data science techniques used, performance metrics, and key findings. The extracted data was organized in a spreadsheet for further analysis.

3. RESULTS

The current systematic review identified a wide range of data science techniques applied in FD (CCF and cyber (online) fraud), including ML algorithms, DL techniques, and hybrid approaches (Table 2). The most commonly used techniques were based on supervised learning algorithms, such as logistic regression (LR), decision trees (DT), and random forests (RT), which were applied in various FD domains, including CCF and cyber (online) fraud. Moreover, unsupervised learning algorithms, such as clustering and anomaly detection techniques, were used to identify suspicious patterns and outliers in financial transactions and CCFs. Furthermore, DL architectures, such as artificial neural networks (ANN) and convolutional neural networks (CNN), demonstrated superior performance in complex FD tasks, particularly in the e-commerce and cyber domain (Btoush et al., 2023; Priscilla & Prabha, 2020).

3.1. Credit Card Fraud Detection

Credit card fraud detection (CCFD) is the technique of categorizing fraudulent transactions as real or fraudulent. The identification of fraudulent activity on a credit card can be accomplished by analyzing the cardholder's spending patterns. Various ML, DL, and AI models have been used for the efficient CCFD. Figure 2 shows the number of studies on CCFD in respective years using ML, DL, and AI techniques.

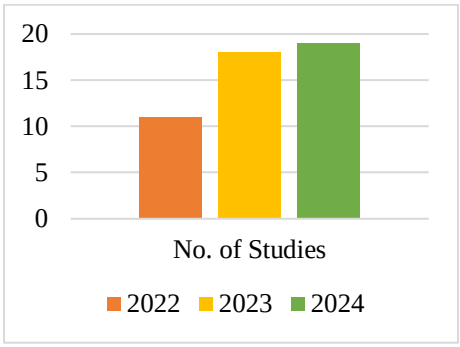

Figure 2. Credit card fraud detection studies during the year 2022-2024.

3.2. ML Techniques in CCFD

Several studies have utilized ML algorithms for CCFD (Table 1). Alarfaj et al. (2022) employed various ML and DL algorithms, achieving high accuracy rates (Alarfaj et al., 2022). Qaddoura&Biltawi (2022) improved FD in imbalanced data using oversampling techniques (Qaddoura & Biltawi, 2022). Roseline et al. (2022) used a Long Short-Term Memory (LSTM) Recurrent Neural Network (LSTM-RNN) (Roseline et al., 2022). Jovanovic et al. (2022) tuned ML models using a Group Search Firefly Algorithm (Jovanovic et al., 2022). Khan et al. (2022) developed a CCFD model using logistic regression, artificial neural networks, and support vector machines (Khan et al., 2022).

Several studies employed ensemble methods, e.g., Sahithi et al. (2022) proposed a predictive classification model using ensemble techniques (Sahithi et al., 2022), and Karthik et al. (2022) combined boosting and bagging for CCFD (Karthik et al., 2022). Khalid et al. (2024) ensembled SVM, KNN, RF, Bagging, and Boosting classifiers (Khalid et al., 2024). Feature engineering techniques were also explored. Kaleel & Polkowski (2023) used SMOTE oversampling with NB, RF, and MLP (Kaleel & Polkowski, 2023), and Noviandy et al. (2023) combined XGBoost with data augmentation (Noviandy et al., 2023). Maithili et al. (2024) used ML with Genetic Algorithm (GA) feature selection (Maithili et al., 2024).

3.3. DL Techniques in CCFD

Some studies utilized DL algorithms for CCFD (Table 1). Alarfaj et al. (2022) employed DL along with ML. Roseline et al. (2022) used an LSTMRNN (Roseline et al., 2022). Fakiha (2023) employed LSTM_DNNs (Fakiha, 2023). Bao et al. (2024) proposed a BERT model with 99.95% accuracy (Bao et al., 2024). Reddy et al. (2024) designed a JNBO-SpinalNet model. Yu et al. (2024) used Transformer models (Reddy et al., 2024).

3.4. Hybrid Techniques in CCFD

Several studies combined ML and DL techniques for CCFD (Table 1). Alarfaj et al. (2022) used a hybrid approach (Alarfaj et al., 2022). Roseline et al. (2022) employed an LSTM-RNN (Roseline et al., 2022). Esenogho et al. (2022) combined SMOTE-ENN with a boosted LSTM (Esenogho et al., 2022). Singh et al. (2023) used a hybrid Fruitfly-Fireworks algorithm with RBF (Singh et al., 2023). Reddy et al. (2024) designed a JNBO-SpinalNet model (Reddy et al., 2024). Yu et al. (2024) used Transformer models and other ML algorithms (Yu et al., 2024). The reviewed studies highlighted several challenges and limitations in applying data science techniques for CCFD. These include

class imbalance (Aftab et al., 2023; Esenogho et al., 2022; Qaddoura & Biltawi, 2022), feature engineering (Cheah et al., 2023; Esenogho et al., 2022; Khan et al., 2022; Rangineni & Marupaka, 2023), and interpretability of complex models (Gill et al., 2023; Singh et al., 2023; Yılmaz, 2023).

Table 1. Data Science tools and models are used for Credit card fraud detection.

Detection of Fraud Type	Year	Title of Study	DOI	Data Science tools			Models used /Findings	References
				ML	DL	Hybrid		
Credit Card Fraud (CCF)	2022	Credit Card Fraud Detection Using State-of-the-art Machine Learning and Deep Learning Algorithms	https://doi.org/10.1109/ACCESS.2022.3166891	✓	✓	✓	Various ML and DL algorithms were used for CCFD.	(Alarfaj et al., 2022)
	2022	Improving fraud detection in an imbalanced class distribution using different oversampling techniques	https://doi.org/10.1109/EICEEAI56378.2022.10050500	✓			ML models such as LR, RF, KNN, NB, SVM, and DT were utilized for CCFD.	(Qaddoura & Biltawi, 2022)
	2022	Autonomous credit card fraud detection using machine learning approach	https://doi.org/10.1016/j.compeleceng.2022.108132	✓			A LSTM-RNN was employed for CCFD.	(Roseline et al., 2022)
	2022	Tuning Machine Learning Models Using a Group Search Firefly Algorithm for Credit Card Fraud Detection	https://doi.org/10.3390/math10132272	✓			GSFA was paired with three standard ML models—SVM, ELM, and XGBoost—and compared with nine others for CCFD.	(Jovanovic et al., 2022)
	2022	Developing a credit card fraud detection model using machine learning approaches		✓			LR, ANN, and SVM were used for CCFD.	(Khan et al., 2022)
	2022	Credit card fraud detection using ensemble methods in machine learning	https://doi.org/10.1109/ICOEI53556.2022.9776955	✓			A predictive classification model was proposed, employing a Weighted Average Ensemble on simple classifiers and classifier ensembles such as LR, RF, KNN, AdaBoost, and Bagging.	(Sahithi et al., 2022)
	2022	Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model	https://doi.org/10.1007/s13369-021-06147-9	✓			Ensemble learning techniques like boosting and bagging were combined for CCFD.	(Karthik et al., 2022)
	2022	A Novel text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach	https://doi.org/10.3390/electronics11050756		✓		The text2IMG-based classification method was applied to CCFD.	(Alharbi et al., 2022)
	2022	A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection	https://doi.org/10.1109/ACCESS.2022.3148298	✓	✓	✓	SMOTE-ENN data resampling combined with a boosted LSTM classifier was found to be efficient for fraud detection.	(Esenogho et al., 2022)
	2022	Credit Card Fraud Prediction Using XGBoost: An Ensemble Learning Approach	https://doi.org/10.4018/IJIRR.299940	✓			XGBoost was used and compared with other ML techniques for CCFD.	(Mohbey et al., 2022)
	2022	Big data analytics for credit card fraud detection using supervised machine learning models	https://doi.org/10.1108/978-1-80262-637-720221003	✓			ML models, including KNN, RC, GB, QDA, AdaBoost, and RF, were employed to classify fraudulent and legitimate transactions.	(Saheed et al., 2022)
	2023	Enhancing Financial Fraud Detection through Addressing Class Imbalance Using Hybrid SMOTE-GAN Techniques	https://doi.org/10.3390/ijfs11030110	✓	✓	✓	The SMOTE and GANs were utilized to address class imbalance issues.	(Cheah et al., 2023)

	2023	A distributed deep neural network model for credit card fraud detection	https://doi.org/10.1016/j.frl.2023.104547		✓		A DDNN was developed to detect credit card fraud.	(Lei et al., 2023)
	2023	Detection of Credit Card Fraud Through Machine Learning in Banking Industry	https://www.jcbi.org/index.php/Main/article/view/204	✓			Various techniques such as Arbitrary Back-woods, SVC, Choice Braid, Neural Organization, and Genetic Calculation were used for CCFD.	(Gill et al., 2023)
	2023	Credit Card Fraud Detection using Neural Embeddings and Radial Basis Network with a novel hybrid fruitfly-fireworks algorithm	https://doi.org/10.1109/CONIT59222.2023.10205378	✓	✓	✓	The Fruitfly Optimization Algorithm (FFFW) and FFO-FWA combined with Radial Basis Function (RBF) were employed for CCFD.	(Singh et al., 2023)
	2023	Forensic Credit Card Fraud Detection Using Deep Neural Network	https://doi.org/10.35741/issn.0258-2724.58.1.33		✓		Sequential data modeling using LSTM Deep Neural Networks (DNNs) was applied for CCFD.	(Fakiha, 2023)
	2023	A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection	https://doi.org/10.33769/aupse.1361266	✓	✓	✓	DT, RF, LR, ANN, NB, and Swarm Optimization were used.	(Yılmaz , 2023)
	2023	Credit card fraud detection using the brown bear optimization algorithm	https://doi.org/10.1016/j.aej.2024.06.040	✓			The Brown-Bear Optimization (BBO) algorithm was used to enhance CCFD.	(Sorour et al., 2024)
	2023	Fraud Detection of Credit Cards Using Supervised Machine Learning Techniques	https://doi.org/10.58619/pjest.v4i3.114	✓			RF was identified as the most suitable supervised ML method for CCFD.	(Aftab et al., 2023)
	2023	Credit-card Fraud Detection System using Neural Networks	https://doi.org/10.34028/iajit/20/2/10	✓	✓	✓	ANN and CNN models were used and assessed with a credit card dataset.	(Al Balawi & Aljohani , 2023)
	2023	Credit Card Fraud Detection and Identification using Machine Learning Techniques	https://doi.org/10.31185/wjcms.228	✓			The SMOTE approach for oversampling was utilized, with NB, RF, and MLP algorithms used for CCFD.	(Kaleel & Polkowski, 2023)
	2023	Credit Card Fraud Detector Based on Machine Learning Techniques	https://doi.org/10.32996/jcsts.2023.5.2.2	✓			SVM, LR, RF, and ANN were used for CCFD.	(Mohsen et al., 2023)
	2023	Analysis of Data Engineering for Fraud Detection Using Machine Learning and Artificial Intelligence Technologies	https://www.doi.org/10.56726/IRJMETS43408	✓	✓	✓	SMOTE, ADASYN, MWMOTE, and ROSE models were employed for fraud detection.	(Rangineni & Marupaka, 2023)
	2023	Detect Fraudulent Transactions Using Credit Cards with Help of ML Algorithms & Deep Learning Algorithms	https://doi.org/10.53555/sfs.v10i2.1436	✓	✓	✓	ML and DL algorithms were used for CCFD.	(Adel & Dubba, 2023)
	2023	A comparison study of fraud detection in usage of credit cards using machine learning	https://doi.org/10.1109/ICOEI56765.2023.10125838	✓	✓	✓	ML techniques such as XGBoost, SVM, DT, RF, and LR were utilized, while CNN was used to improve CCFD efficiency.	(Prasad et al., 2023)
	2023	Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques	https://doi.org/10.60084/ijma.v1i1.78	✓			XGBoost and data augmentation techniques enhanced CCFD.	(Novian dy et al., 2023)

	2023	Uncertainty-aware credit card fraud detection using deep learning	https://doi.org/10.1016/j.engappai.2023.106248		✓		Three uncertainty quantification (UQ) techniques, Monte Carlo dropout, ensemble, and ensemble Monte Carlo dropout, were proposed for CCFD.	(Habibpour et al., 2023)
	2023	Fraud Detection and Identification in Credit Card Based on Machine Learning Techniques	https://doi.org/10.31185/wjcms.185	✓			NB, RF, and MLP algorithms were used for CCFD.	(Unogwu & Filali, 2023)
	2023	Credit card fraud detection using predictive features and machine learning algorithms	https://doi.org/10.1504/IJITST.2023.129578	✓			RF and ML algorithms, such as SVM IF, were used for CCFD.	(Rtayli & Enneya, 2023)
	2024	Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach	https://doi.org/10.3390/bdcc8010006	✓			Ensemble methods combining SVM, KNN, RF, Bagging, and Boosting classifiers were employed for effective CCFD.	(Khalid et al., 2024)
	2024	Application of Deep Learning in Financial Credit Card Fraud Detection	https://doi.org/10.5281/zenodo.10960092		✓		A BERT model with 99.95% accuracy was proposed for CCFD.	(Bao et al., 2024)
	2024	Development of an efficient machine learning algorithm for reliable credit card fraud identification and protection systems	https://doi.org/10.1051/matecconf/202439201116	✓			EMLA-RCCFI, using ML and GA for feature selection, was constructed for CCFD.	(Maithili et al., 2024)
	2024	Deep learning-based credit card fraud detection in federated learning	https://doi.org/10.1016/j.eswa.2024.124493		✓		The JNBO-SpinalNet model was designed for CCFD.	(Reddy et al., 2024)
	2024	Credit Card Fraud Detection Using Machine Learning Techniques	https://doi.org/10.4236/jcc.2024.126001	✓			Four ML classifiers—SVM, DT, NB, and RF—were used for CCFD.	(Sarker et al., 2024)
	2024	Probabilistic Deep Learning Approach to Credit Card Fraud Detection	https://doi.org/10.1109/MIPRO60963.2024.10569683		✓		The algorithm was tested on a synthetic transaction dataset for CCFD.	(Mrčela & Kostanjčar, 2024)
	2024	Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements	https://doi.org/10.1016/j.future.2024.04.057	✓			BFL and ML models were applied to local data for CCFD.	(Chatterjee et al., 2024)
	2024	Credit Card Fraud Detection Using Advanced Transformer Model	https://doi.org/10.48550/arXiv.2406.03733	✓			Transformer models were used and compared with SVM, RF, NN, LR, XGBoost, and TabNet for more robust and precise CCFD.	(Yu et al., 2024)Yu, et al.
	2024	An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection	https://doi.org/10.1109/TAI.2024.3359568		✓		An RTAHC model based on deep reinforcement learning was proposed for CCFD.	(Zhu et al., 2024)
	2024	Detection of Credit Card Fraud with Optimized Deep Neural Network in Balanced Data Condition	https://doi.org/10.7494/csci.2024.25.2.5967		✓		A hyper-model consisting of NN and DT/SVM was developed for a robust and efficient CCFD model.	(Shome et al., 2024)
	2024	A novel approach for credit card fraud transaction detection using deep reinforcement learning schema	https://doi.org/10.7717/peerj-cs.1998		✓		The Deep Q Network was proposed for real-time CCFD.	(Qayoom et al., 2024)

	2024	Encoder–decoder graph neural network for credit card fraud detection	https://doi.org/10.1016/j.jksuci.2024.102003	✓			GNNs were used for efficient CCFD.	(Cherif et al., 2024)
	2024	Credit Card Fraud Detection using Deep Learning and Machine Learning Algorithms	https://doi.org/10.56536/jicet.v4i1.106	✓	✓		Six ML algorithms were tested, with RF and Extra Trees Classifier (ETC) being the best. For Neural Networks, LSTM performed best.	(Zahid et al., 2024)
	2024	Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection	https://doi.org/10.47709/cnahpc.v6i2.3814	✓			The study compared traditional and advanced ML models, including LR, SVM, RF, GB, KNN, NB, AdaBoost, LightGBM, XGBoost, and MLP, finding XGBoost to be the most effective.	(Airlangga, 2024)
	2024	Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms	https://doi.org/10.7717/peerj-cs.2088	✓	✓	✓	A novel approach was proposed for fraud detection using CNNs with SVM, KNN, NB, and DT algorithms.	(Ming et al., 2024)
	2024	AI Based Credit Card Fraud Detection using Machine Learning Technique		✓	✓	✓	The proposed LR-based classifier outperformed commonly used classifiers like the vote and KNN, with a 97.2% accuracy rate.	(B. R. Kumar, 2024)
	2024	Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA	https://doi.org/10.32996/jcsts.2024.6.2.1	✓	✓	✓	Four models—SVM, LR, RF, and ANN—were tested for CCFD, with ANN being the most precise using a large dataset.	(Hasan et al., 2024)
	2024	Credit Card Fraud Detection using KNN, Random Forest and Logistic Regression Algorithms: A Comparative Analysis		✓			Random Forest, K-Nearest Neighbor, and Logistic Regression models exhibited remarkable accuracy for CCFD.	(Saeed & Abdulazeez, 2024)
	2024	CaT-GNN: Enhancing Credit Card Fraud Detection via Causal Temporal Graph Neural Networks	https://doi.org/10.48550/arXiv.2402.14708			✓	A novel method, CaTGNN, was proposed for CCFD and showed superior performance compared to existing state-of-the-art methods.	(Duan et al., 2024)

Table 2. Advantages and Disadvantages of Different ML/ DL and AI approaches in CCFD.

Algor.	**Advantages**	**Disadvantages**
DT	- Easy to interpret and understand decisions. - Handles both numerical and categorical data well. - Automatically handles missing values and feature selection.	- Prone to overfitting, especially with complex trees. - Can create biased trees if some classes dominate the data.
LR	- Simple and efficient for binary classification. - Outputs probabilities for outcomes.	- Assumes a linear relationship between features and outcomes. - Sensitive to outliers and multicollinearity.
KNN	- Intuitive and simple to implement. - Robust to noisy data and irrelevant features.	- Computationally expensive for large datasets or many features. - Sensitive to the choice of distance metric and *k*k value.
NN	- Ability to capture complex patterns in data. - Adaptable to diverse data types.	- Prone to overfitting, especially with insufficient data. - Computationally expensive and requires substantial computing power and time for training.
ANN	- Suitable for complex pattern recognition. -Can model nonlinear relationships in data.	- Prone to overfitting with large networks and training data. - Requires a large amount of data for effective training. - Complex architectures can be hard to interpret.

NB	- Simple and fast for classification tasks. - Efficient with high-dimensional data.	- Assumes independence between features, which can limit performance in cases of strong dependencies. - Sensitive to irrelevant features and the presence of rare combinations of features in the training data.
GA	- Effective in exploring large solution spaces and finding near-optimal solutions. - Suitable for optimization problems with many parameters.	- Computationally expensive for complex problems and large datasets. - Initialization and parameter tuning can significantly impact performance.
Isolation Forest	- Effective for anomaly detection. - Works well with high-dimensional data.	- Not effective for small datasets. - Requires careful parameter tuning.
HMM	- Ability to model sequential data and hidden states. - Efficient for time-series analysis.	- Sensitive to the choice of the number of hidden states. - Assumes Markov property (independence of future states given the present), which might not always hold true in real-world scenarios.
AIS	- Various uses, including the discovery of false financial transactions. - AIS discovery engines can categorize input data as genuine or fake.	- Limited research and application in fraud detection. - Can be complex to implement and understand.
CT	- Effective for breakpoint assessment in financial transactions. - Can recognize dubious activities based on transaction patterns.	- Limited generalizability across different types of fraud. - Domain-specific knowledge may be required for effective implementation.
ILP	- Suitable for constructing classifiers for social datasets. - Can handle complex relational data.	- Limited scalability for large datasets. - Can be difficult to implement and interpret.
OD	- Effective for identifying anomalies and unusual patterns. - Can be used for extortion recognition.	- May generate false positives if not properly tuned. - Domain expertise is required for effective anomaly detection.
SVM	- Effective in high-dimensional spaces. - Versatile due to different kernel functions.	- Computationally intensive for large datasets. - Difficult to interpret complex models. - Sensitive to the choice of kernel and regularization parameters.
FLBS	- Suitable for handling imprecise and uncertain data. - Can represent linguistic terms and expert knowledge in a structured manner.	- Interpretability can be challenging with complex fuzzy systems. - Requires careful design of fuzzy rules, which might need domain expertise. - Complex systems might suffer from scalability issues and increased computational complexity.
CNN	- Highly effective for image and spatial data. - Can automatically detect important features without human intervention.	- Large amounts of labelled data are required for training. - Computationally expensive and requires significant processing power.
XGBoost	- Powerful open-source implementation of gradient boosting. - Effective for a wide range of prediction tasks. - Combines multiple weak models to improve accuracy.	- Can be computationally intensive. - Requires careful parameter tuning to avoid overfitting. - Complex models can be hard to interpret.
Voting Classifier	- Improves model performance by combining multiple classifiers. - Versatile and can be applied to various types of data.	- Complexity in parameter tuning and integration of multiple models. - May suffer from interpretability issues when combining diverse methods. - Potential scalability and computational resource issues when incorporating multiple techniques.
LSTM	- Effective for modelling sequential and time-series data. - Can capture long-term dependencies in data.	- Computationally expensive and requires large datasets for training. - Can be difficult to tune and interpret.

BERT	- State-of-the-art for natural language processing tasks. - Pre-trained models can be fine-tuned for specific tasks with relatively small datasets.	- Computationally expensive and requires significant memory. - Complex architecture can be difficult to interpret and implement.
Hybrid Approaches	- Combines strengths of different methods for better performance. - Offers versatility and adaptability.	- Complexity in parameter tuning and integration of multiple models. - May suffer from interpretability issues when combining diverse methods. - Potential scalability and computational resource issues when incorporating multiple techniques.

3.5. Cyber (Online) Fraud Detection

Traditional cyber fraud detection (CFD) methods are becoming inadequate due to the evolving nature of cyber threats. ML and artificial intelligence have emerged as promising technologies for improving detection capabilities. Over time, they can learn from data to adapt to new threats(Cao et al., 2024). Some key ways AI and ML are used for CFD include proactive threat detection, real-time analysis, anomaly detection, threat intelligence analysis, and behavior-based analysis. Proactive detection uses patterns in logs and traffic to find subtle threats, including zero-days. Real-time analysis allows machines to rapidly process large data volumes, improving response times(Btoush et al., 2023).

Anomaly detection sets up standard patterns and alerts on potential intrusions to the system. Threat intelligence analysis is a way of combining information gathered internally and externally in order to look for patterns and potential attacks. Behavioral analysis techniques focus on how an entity communicates with the networks to identify insiders or the movement of the threats. Both AI and ML are also used to detect malware. It can teach them new patterns and codes to detect the new strains of malware, such as polymorphic and file-less malware, that are hard to detect by signature-based tools. Such threats are easily identifiable by the ML algorithms even when other methods are not useful. The second major application involves the ability to respond to an incident automatically. AI can automate response workflows to contain infected systems, stop communication with the source, and start investigations. This decreases the workload of security personnel while guaranteeing prompt and uniform responses that contain the impact of threats (Barraclough et al., 2021; Minastireanu & Mesnita, 2019).

Table 3. Data Science tools and models are used for Credit card fraud detection.

Detection of Fraud Type	**Year**	**Title**	**DOI**	**Data Science tools**			**Model Used/findings**	**References**
				ML	**DL**	**Hybrid**		
Cyber (online) fraud	2022	An intelligent cyber security phishing detection system using deep learning techniques	https://doi.org/10.1007/s10586-022-03604-4		✓		They used Locally-deep SVM, SVM, Boosted DT, LR, AP, NN, and DF algorithms. Boosted DT and DF were found to be more accurate and precise.	(Mughaid et al., 2022)
	2022	A predictive model for phishing detection	https://doi.org/10.1016/j.jksuci.2019.12.005	✓			They used SVM and NB, trained on a 15-dimensional feature set, for phishing detection.	(Orunsolu et al., 2022)
	2022	Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection	https://doi.org/10.1155/2022/1424638	✓			They proposed and used KNN and a density-based algorithm to detect fraudulent documents (FDs) more accurately than other ML algorithms.	(Du et al., 2022)
	2022	Visual similarity-based phishing detection using deep learning	https://doi.org/10.1117/1.JEI.3		✓		They addressed visual similarity issues related to computer vision, such as webpage segmentation	(Saeed, 2022)

	2		1.5.05160 7				and feature extraction, for phishing detection.	
	2 0 2 3	Click fraud detection for online advertising using machine learning	https://doi .org/10.10 16/j.eij.20 23.05.006	✓			They applied ML models to determine whether a website visitor is a human or an automated bot user to detect Pay-per-click online fraud.	(Aljabri & Moham mad, 2023)
	2 0 2 3	Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification	https://doi .org/10.58 346/JISIS. 2023.I4.0 10		✓		A Deep Fraud Net (DFN) was used to effectively detect and categorize instances of fraudulent behavior with reduced misclassifications.	(Udayak umar et al., 2023)
	2 0 2 3	The advanced proprietary AI/ML solution as Anti-fraudTensorlink4cheque (AFTL4C) for Cheque fraud detection	https://hco mmons.or g/deposits /item/hc:5 4851	✓	✓	✓	They used a GAN-based Anti-fraud-Tensorlink4cheque (AFTL4C) solution for real-time FD.	(Uyyala & Yadav, 2023)
	2 0 2 3	Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework	https://doi .org/10.10 07/s10796 -022-10346-6	✓			They employed a semi-supervised ensemble model and an XGBoost classifier for FD in mobile payments.	(Hajek et al., 2023)
	2 0 2 3	Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers	http://dx.d oi.org/10. 32604/css e.2023.02 6508				They used ML algorithms such as DT, RF, LR, and GB to detect and predict fraud cases.	(Valava n & Rita, 2023)
	2 0 2 3	Safeguarding against Cyber Threats: Machine Learning-Based Approaches for Real-Time Fraud Detection and Prevention	https://doi .org/10.33 90/engpro c2023059 111	✓			They used DL techniques and ANN to detect complex fraud patterns, while LR was used for typical fraudulent event probability assessment.	(Shetty & Malgha n, 2023)
	2 0 2 3	Modelling of an Adaptive Network Model for Phishing Website Detection Using Learning Approaches	https://doi .org/10.54 216/FPA.1 20213		✓		They compared various DL models and achieved the highest accuracy of 99.18% with the adaptive Recurrent Neural Networks model.	(Tenis & Santhos h, 2023)
	2 0 2 3	AI-based model for fraud detection in bank systems	https://doi .org/10.54 216/FPA.1 40102			✓	They used Genetic Algorithms (GA) to detect false financial transactions and improve intrusion detection systems.	(Al-Fatlawi et al., 2024)
	2 0 2 3	Machine Learning-Based Intrusion Detection System for Cyber Attacks in Private and Public Organizations	https://doi .org/10.30 534/ijsait/ 2023/0312 52023	✓			They used RF and RT algorithms for cyber fraud and found precision and F-measure levels to be above 99% and 98%, respectively.	(Emman uel et al., 2023)
	2 0 2 3	Machine Learning-Driven Detection and Prevention of Cryptocurrency Fraud	https://doi .org/10.11 09/RMK MATE592 43.2023.1 0369055	✓			Among ML techniques for cryptocurrency fraud, they found that XGBoost had the best accuracy at 98%, followed by AdaBoost at 67% and RF at 90%.	(Sharma & Babbar, 2023)
	2 0 2 3	Online payment fraud: from anomaly detection to risk management	https://doi .org/10.11 86/s40854 -023-00470-w	✓			They used an ML triage model for online payment fraud and found it reduced expected losses by 52%.	(Vanini et al., 2023)
	2 0	Online Payment Fraud Detection Model Using	https://doi .org/10.11	✓			They used the Jaya optimization algorithm (RXT-J) for online	(Almazr oi &

	23	Machine Learning Techniques	09/ACCESS.2023.3339226				payment fraud detection.	Ayub, 2023)
	2023	An ensemble fraud detection approach for online loans based on application usage patterns	https://doi.org/10.3233/JIFS-222405	✓	✓		They designed the Grouped Trees and Weighted Ensemble (GTWE) algorithm for fraud detection in online loan applications.	(Xu et al., 2023)
	2023	An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures	https://doi.org/10.48084/etasr.6401	✓			They proposed an ensembling approach (Stacking model) for fraud detection systems.	(Alhashmi et al., 2023)
	2023	A Powerful Predicting Model for Financial Statement Fraud Based on Optimized XGBoost Ensemble Learning Technique	https://doi.org/10.3390/app13042272	✓			They proposed the FSF model using the XGBoost algorithm for FD in the MENA region.	(Ali et al., 2023)
	2023	Identification of Phishing Attacks using Machine Learning Algorithm	https://doi.org/10.1051/e3sconf/202339904010	✓			They used ML algorithms such as RF, XGBoost, and LR to detect real or phishing websites.	(Dinesh et al., 2023)
	2024	Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning	https://doi.org/10.3389/fcomp.2024.1428013	✓			They evaluated and compared 15 SML algorithms from different ML families and ensembles for phishing attacks.	(Tamal et al., 2024)
	2024	Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification	https://doi.org/10.1016/j.frl.2023.104843	✓			They designed and used self-attention Generative Adversarial Networks (SAGANs) to detect complex cyber fraud.	(Zhao et al., 2024)
	2024	Combatting Online Fraud: Advancing Fraud Detection in Internet Loans through Deep Learning Innovations			✓		They focused on developing a DL-based anti-fraud ANN model for Internet loan applications.	(Kumar et al., 2024)
	2024	Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning	https://doi.org/10.32996/jcsts.2024.6.1.19			✓	They used Feedzai's AI-based software combined with RF algorithms to achieve real-time fraud detection in financial institutions.	(Labu & Ahammed, 2024)
	2024	Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks	https://doi.org/10.1108/DPRG-02-2024-0029	✓			ML-based data analysis using self-organizing maps was employed to assess the severity of cyber fraud dynamically and in real time.	(Chhabra Roy & P, 2024)
	2024	Cybersecurity threats in banking: Unsupervised fraud detection analysis	https://doi.org/10.30574/ijsra.2024.11.2.0505	✓	✓		They used modern ML algorithms to reduce cybersecurity threats and ensure the security of digital transactions in the banking industry.	(Meduri, 2024)
	2024	Fraud Detection in NoSQL Database Systems using Advanced Machine Learning	https://doi.org/10.38124/ijisrt/IJISRT24MAR127	✓			They used ML techniques to enhance fraud and intrusion detection in NoSQL databases.	(Arjunan, 2024)

	2024	A comparative analysis of various machine learning methods for anomaly detection in cyber-attacks on IoT networks	https://doi.org/10.1016/j.iot.2024.101162	✓			The comparative analysis included various ML techniques, such as SVM, ANN, DT, LR, and KNN. The results showed that the neural network performed better than the other models.	(Inuwa & Das, 2024)
	2024	Application of Machine Learning-Based K-means Clustering for Financial Fraud Detection	https://doi.org/10.54097/74414c90	✓			They found that the ML-based K-means clustering method effectively detects financial fraud.	(Huang et al., 2024)
	2024	Advanced Cybercrime Detection: A Comprehensive Study on Supervised and Unsupervised Machine Learning Approaches Using Real-world Datasets	https://doi.org/10.32996/jcsts.2024.6.1.5	✓			They used SVM and KNN models for cybercrime detection, with SVM achieving a 91% accuracy rate.	(Cao et al., 2024)
	2024	Leveraging Machine Learning for Enhanced Cyber Attack Detection and Defence in Big Data Management and Process Mining	https://doi.org/10.14569/ijacsa.2024.0150266	✓			They used ML techniques to detect and defend against cyber threats within big data management and process mining.	(Gongada et al., 2024)
	2024	Cybersecurity Threat Detection using Machine Learning and Network Analysis	https://doi.org/10.60087/jaigs.v1i1.88	✓			They proposed a novel approach to balance energy savings and system security in Cyber-Physical Systems (CPSs).	(A. Kumar, 2024)
	2024	Enhancing Cybersecurity: Machine Learning Approaches for Predicting DDoS Attack	https://doi.org/10.56532/mjsat.v4i3.306	✓			Researchers used the CIC-DDoS2019 dataset to analyze DDoS attack frequencies and patterns on servers.	(Ferdous et al., 2024)
	2024	Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia	https://doi.org/10.3390/electronics13050824	✓			They used LR, NB, and KNN algorithms for cyberattack prevention in Colombia's IoT infrastructure.	(Ortiz-Ruiz et al., 2024)
	2024	Cybersecurity Threats Detection Using Optimized Machine Learning Frameworks	https://doi.org/10.32604/csse.2023.039265	✓			They compared PSO-SVM with other methods, such as KNN, DT, and ANN, finding PSO-SVM to be superior.	(Omer et al., 2024)
	2024	Intrusion detection based on phishing detection with machine learning	https://doi.org/10.1016/j.measen.2023.101003	✓			They proposed a Hybrid Ensemble Feature Selection (HEFS) method for ML-based phishing detection systems.	(Jayaraj et al., 2024)
	2024	Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security	https://doi.org/10.1016/j.csa.2023.100033	✓			They applied five popular classification algorithms to a full training dataset and found that the J48 algorithm achieved a good accuracy of 79.1%.	(Nabi & Zhou, 2024)
	2024	An Intrusion System for Internet of Things Security Breaches Using Machine Learning Techniques	https://doi.org/10.47852/bonviewAIA42021780	✓			They used the Densenet201 model to categorize attacks across datasets, including Bot-IoT, CICIDS2017, and CICIDS2019, through Data Processing (DP) methodologies.	(Adekunle et al., 2024)

	2024	Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features	https://doi.org/10.3390/info15010036	✓			They employed time-series forecasting techniques, including SMO regression, LR, and LSTM, to construct and tune time-series models for forecasting cyber events.	(Ahmed et al., 2024)
	2024	Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks	https://doi.org/10.1016/j.iot.2023.101012	✓			The results indicated that ML algorithms underperformed under cyber-attacks, leading to a significant decrease in the accuracy of transient stability predictions compared to normal operating conditions.	(Aygul et al., 2024)

The studies included in this review have employed various ML and DL techniques to detect cyber and online fraud (Figure 3). The key findings and methodologies are summarized in the following subsections (Table 3).

3.6. Machine Learning Techniques in CFD

Several studies have utilized ML algorithms for cyber and online fraud detection. Mughaid et al. (2022) used Locally-deep SVM, SVM, Boosted DT, LR, AP, NN, and DF algorithms, finding Boosted DT and DF to be more accurate and precise for phishing detection. Orunsolu et al. (2022) used SVM and NB trained on a 15-dimensional feature set for phishing detection. Du et al. (2022) proposed and used KNN and density-based algorithms to detect ransomware more accurately than other ML algorithms. Aljabri& Mohammad (2023) applied ML models to determine whether a website visitor is human or bot to detect pay-per-click online fraud. Valavan & Rita (2023) used ML algorithms such as DT, RF, LR, and GB for fraud detection and prediction. Sharma & Babbar (2023) found XGBoost to have the best accuracy at 98%, followed by AdaBoost and RF, for cryptocurrency fraud detection. Vanini et al. (2023) used an ML triage model for online payment fraud, reducing expected losses by 52%. Almazroi& Ayub (2023) used the Jaya optimization algorithm (RXT-J) for online payment fraud detection. Dinesh et al. (2023) used RF, XGBoost, and LR for phishing website detection. Tamal et al. (2024) evaluated and compared 15 supervised ML algorithms and ensembles for phishing attack detection. Labu & Ahammed (2024) used Feedzai's AI-based software and RF algorithms for real-time fraud detection in financial institutions. Chhabra Roy and co-workers (2024) used ML-based data analysis with self-organizing maps to dynamically and in real-time assess the severity of cyber fraud. Inuwa & Das (2024) performed a comparative analysis of ML techniques, including SVM, ANN, DT, LR, and KNN, finding neural networks performed better than other models for anomaly detection in IoT network cyber-attacks.

Cao et al. (2024) used SVM and KNN models for cybercrime detection, with SVM achieving a 91% accuracy rate. Ortiz-Ruiz et al. (2024) used LR, NB, and KNN algorithms for cyberattack prevention in Colombia's IoT infrastructure. Omer et al. (2024) proposed and compared PSO-SVM with other approaches, such as KNN, DT, and ANN, achieving better results with PCO-SVM for cybersecurity threat detection. Nabi & Zhou (2024) used five popular classification algorithms, finding the J48 algorithm attained a relatively good accuracy of 79.1% for intrusion detection system enhancement through dimensionality reduction. Adekunle et al. (2024) used the Densenet201 model to categorize attacks across various IoT security datasets. Ahmed et al. (2024) used time-series forecasting techniques, including SMOreg, LR, and LSTM, to forecast cyber events. Aygul et al. (2024) found that under cyber-attacks, ML algorithms underperform, leading to a significant decrease in the accuracy of transient stability predictions in renewable-rich power grids.

3.7. Deep Learning Techniques in CFD

Some studies utilized DL algorithms for cyber and online fraud detection. Saeed (2022) used visual similarity-based deep learning for phishing detection, which raises several computer vision-related issues. Udayakumar et al. (2023) used a DFN to effectively detect and categorize instances of fraudulent behavior with reduced misclassifications. Uyyala& Yadav (2023) used a GAN-based Anti-fraud-Tensorlink4cheque (AFTL4C) solution for real-time fraud detection. Shetty &Malghan (2023) used DL techniques and ANN to detect complex fraud patterns, while LR was

typical of the probability of fraudulent events. Tenis & Santhosh (2023) compared various DL models and achieved the greatest accuracy of 99.18% using an adaptive Recurrent Neural Networks model for phishing website detection. Xu et al. (2023) designed the grouped trees and weighted ensemble algorithm (GTWE) for fraud detection in online loan applications. Zhao et al. (2024) designed and used self-attention generative adversarial networks (SAGANs) to detectCCF. Kumar et al. (2024) focused on developing a DL anti-fraud ANN model for Internet loan applications. Meduri (2024) used modern ML algorithms to reduce cybersecurity threats and ensure the security of digital transactions within the banking industry.

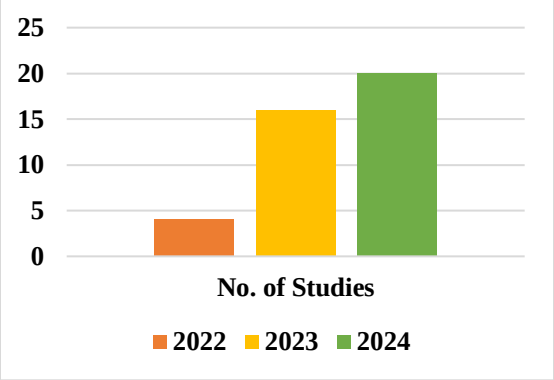

Figure 3. Cyber (online) fraud detection studies in each year.

4. DISCUSSION

The review highlights the effectiveness of various data science techniques in detecting fraudulent activities. ML algorithms, particularly supervised learning methods, have been widely adopted due to their ability to learn from historical data and make predictions on unseen instances. Studies have shown that algorithms such as LR, DTs, RFs, and SVMs are commonly employed in fraud detection tasks. For example, Alarfaj et al. (2022) demonstrated that a combination of ML and DL algorithms significantly improved the accuracy of CCFD. DL techniques have also gained traction, particularly in complex fraud detection scenarios where traditional methods may fall short. The ability of deep learning models, such as LSTM networks and CNNs, to capture intricate patterns in large datasets has proven beneficial in domains like e-commerce and cyber (online) fraud detection(Alarfaj et al., 2022). For instance, Fakiha (2023) employed LSTM networks for sequential data modeling, achieving impressive results in detecting fraudulent transactions. Hybrid approaches combining ML and DL techniques have emerged as a promising avenue for enhancing fraud detection capabilities. By leveraging the strengths of both methodologies, researchers have developed models that can effectively handle diverse fraud scenarios(Fakiha, 2023). For example, Singh et al. (2023) utilized a hybrid Fruitfully-Fireworks algorithm with radial basis function networks, achieving superior performance in CCFD(Singh et al., 2023).

4.1. Challenges in Fraud Detection

Despite the advancements in data science techniques, several challenges persist in the realm of FD. Among the most pressing problems, one can mention the class imbalance problem, in which fraudulent instances may be much fewer than legitimate transactions. Such an imbalance can result in skewed models favoring the perpetrators of fraud in that their fraudulent activities are not detected. Other previous works, for instance, Aftab et al., 2023, and Qaddoura&Biltawi, 2022, have proposed oversampling and synthetic data generation to overcome this problem, while there is a need for more research in this area. Another issue is the explainability of intricate models. Indeed, deep learning algorithms can provide very accurate results, but at the same time, they are 'black boxes,' thus not allowing the stakeholders to understand the decision-making process. Such lack of transparency is detrimental to the models in terms of trust and the subsequent incorporation of the models into practical use (Aftab et al., 2023; Qaddoura & Biltawi, 2022). As Gill et al. (2023) and Singh et al. (2023) have pointed out, investing in methods that would improve the explainability of AI models and boost people's trust is crucial. Also, the dynamic nature of fraud schemes constitutes a threat to detection systems, as fraudsters quickly develop new strategies (Gill et al., 2023;

Singh et al., 2023). There is always an evolution in the fraudster tactics, meaning the models must be updated and retrained frequently. The constantly evolving nature of fraud means that it is necessary to have algorithms capable of learning from new data and updating their models.

4.2. Emerging Trends

The review also outlines several trends noted in the literature on FD. Another trend is using AI methods, including reinforcement learning and GANs, in FD systems, for example. These techniques are more sophisticated and provide new ways of dealing with complicated fraud cases and increasing the efficiency of the detection process. For example, GANs, in the case of data generation, can be used to solve problems associated with class imbalance and improve model training. Another trend is the increasing interest in real-time FD. Due to the growth of Internet transactions, the need to have real-time detection tools for fraud has become crucial. Scholars are investigating ways of creating models that can process the transaction information in real-time and give real-time alarms for any unlawful activities. This change in real-time detection aligns with the growing demand of consumers and businesses for quick responses to fraud.

Moreover, it is also evident that there is a focus on the cooperation of different players, such as financial institutions, regulatory bodies, and technology solutions to fight fraud effectively. It is also important to note that joint projects can result in the exchange of information and, therefore, increase the efficiency of FD systems. This approach is especially suitable for cyber fraud because the systems are interconnected, and a coordinated response should be provided to new threats.

4.3. Future Research Directions

The findings of this review highlight several areas for future research in FD. Firstly, there is a lack of sufficient research that compares the effectiveness of the various algorithms used in the different fraud domains. Cross-sectional studies can be useful because they illustrate the advantages and disadvantages of particular methodologies, which can help practitionerschoose the right techniques for their work. Secondly, future studies should be directed toward creating mixed models, which will enhance the features of the ML and the DL approaches and minimize their drawbacks, such as the interpretability of the models and the problem of the imbalanced classes. The measures that will be valuable for building trust with stakeholders will be the new strategies that help increase model interpretability and give reasons for the output data. Furthermore, the further study of FD systems' integration with advanced technologies like blockchain and federated learning remains relevant. Blockchain helps secure and improve data quality, while federated learning helps train models without sharing the data. Studying these technologies' prospects can inform the development of more effective and secure FD solutions. Finally, the effects of the regulatory changes and changes in the consumers' behaviours regarding FD practices should be explored. Given the dynamic nature of rules regarding data privacy and security, researchers need to determine how these changes impact FD strategies and the implementation of new technologies.

5. CONCLUSION

This systematic review aims to present the findings of a scoping of the current state of research on data science applications in FD. The study also shows the possibility of applying ML and DL methods to improve FD performance in different fields. However, the review also points to issues that have to do with these techniques and their drawbacks, such as data imbalance, lack of labeled data, and interpretability of intricate models. The review also reinforces the need to include domain knowledge and context alongside traditional data science and machine learning paradigms and the possibility of integrating two or more approaches. Potential areas for future research include the study of federated learning, methods aimed at preserving privacy, and the development of explainable AI. The knowledge derived from this review can help researchers and practitioners design improved and efficient FD systems that employ data science approaches. The future of data science-based FD can be further developed by addressing the identified challenges and focusing on the discussed trends, thus helping establish a safer environment for businesses and consumers.

DECLARATIONS

All authors declare that they have no conflicts of interest.

REFERENCES

[1] Abed, M., & Fernando, B. (2023). E-commerce fraud detection based on machine learning techniques: Systematic literature review. Big Data Min. Anal.

[2] Adekunle, T. S., Alabi, O. O., Lawrence, M. O., Adeleke, T. A., Afolabi, O. S., Ebong, G. N., Egbedokun, G. O., & Bamisaye, T. A. (2024). An intrusion system for internet of things security breaches using machine learning techniques. Artificial Intelligence and Applications,

[3] Adel, M., & Dubba, N. M. (2023). Detect Fraudulent Transactions Using Credit Cards with Help of ML Algorithms & Deep Learning Algorithms. Journal of Survey in Fisheries Sciences, 829-834.

[4] Aftab, A., Shahzad, I., Anwar, M., Sajid, A., & Anwar, N. (2023). Fraud Detection of Credit Cards Using Supervised Machine Learning. Pak. J. Emerg. Sci. Technol. (PJEST), 4, 38-51.

[5] Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features. Information, 15(1), 36.

[6] Airlangga, G. (2024). Evaluating the Efficacy of Machine Learning Models in Credit Card Fraud Detection. Journal of Computer Networks, Architecture and High-Performance Computing, 6(2), 829-837.

[7] Al-Fatlawi, A., Al-Khazaali, A. A. T., & Hasan, S. H. (2024). AI-based model for fraud detection in bank systems. Journal of Fusion: Practice and Applications, 14(1), 19-27.

[8] Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.

[9] Al Balawi, S., & Aljohani, N. (2023). Credit-card fraud detection system using neural networks. Int. Arab J. Inf. Technol., 20(2), 234-241.

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

[11] Alharbi, A., Alshammari, M., Okon, O. D., Alabrah, A., Rauf, H. T., Alyami, H., & Meraj, T. (2022). A novel text2IMG mechanism of credit card fraud detection: A deep learning approach. Electronics, 11(5), 756.

[12] Alhashmi, A. A., Alashjaee, A. M., Darem, A. A., Alanazi, A. F., & Effghi, R. (2023). An ensemble-based fraud detection model for financial transaction cyber threat classification and countermeasures. Engineering, Technology & Applied Science Research, 13(6), 12433-12439.

[13] Ali, A. A., Khedr, A. M., El-Bannany, M., & Kanakkayil, S. (2023). A powerful predicting model for financial statement fraud based on optimized XGBoost ensemble learning technique. Applied Sciences, 13(4), 2272.

[14] Aljabri, M., & Mohammad, R. M. A. (2023). Click fraud detection for online advertising using machine learning. Egyptian Informatics Journal, 24(2), 341-350.

[15] Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. IEEE Access, 11, 137188-137203.

[16] Arjunan, T. (2024). Fraud Detection in NoSQL Database Systems Using Advanced Machine Learning. International Journal of Innovative Science and Research Technology(IJISRT), March, 13, 248-253.

[17] Ashley Kilroy. (2024, Mar 21, 2024). Insurance Fraud Statistics 2024. Forbes. Retrieved 28th June 2024 from https://www.forbes.com/advisor/insurance/fraud-statistics/

[18] Aygul, K., Mohammadpourfard, M., Kesici, M., Kucuktezcan, F., & Genc, I. (2024). Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks. Internet of Things, 25, 101012.

[19] Bao, Q., Wei, K., Xu, J., & Jiang, W. (2024). Application of Deep Learning in Financial Credit Card Fraud Detection. Journal of Economic Theory and Business Management, 1(2), 51-57.

[20] Barraclough, P. A., Fehringer, G., & Woodward, J. (2021). Intelligent cyber-phishing detection for online. computers & security, 104, 102123.

[21] Benedek, B., & Nagy, B. Z. (2023). Traditional versus AI-Based Fraud Detection: Cost Efficiency in the Field of Automobile . Financial and Economic Review, 22(2), 77-98.

[22] Berg, H. H., & Hansen, S. E. (2020). The stock market effect of Cybercriminals: an empirical study of the price effects on US listed companies targeted by a data breach

[23] Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.

[24] Cao, D. M., Sayed, M. A., Islam, M. T., Mia, M. T., Ayon, E. H., Ghosh, B. P., Ray, R. K., & Raihan, A. (2024). Advanced cybercrime detection: A comprehensive study on supervised and unsupervised machine learning approaches using real-world datasets. Journal of Computer Science and Technology Studies, 6(1), 40-48.

[25] Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems.

[26] Cheah, P. C. Y., Yang, Y., & Lee, B. G. (2023). Enhancing financial fraud detection through addressing class imbalance using hybrid SMOTE-GAN techniques. International Journal of Financial Studies, 11(3), 110.

[27] Cherif, A., Ammar, H., Kalkatawi, M., Alshehri, S., & Imine, A. (2024). Encoder–decoder graph neural network for credit card fraud detection. Journal of King Saud University-Computer and Information Sciences, 36(3), 102003.

[28] Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. Digital Policy, Regulation and Governance.

[29] Dinesh, P., Mukesh, M., Navaneethan, B., Sabeenian, R., Paramasivam, M., & Manjunathan, A. (2023). Identification of phishing attacks using machine learning algorithm. E3S Web of Conferences,

[30] Du, J., Raza, S. H., Ahmad, M., Alam, I., Dar, S. H., & Habib, M. A. (2022). Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. Security and Communication Networks, 2022(1), 1424638.
[31] Duan, Y., Zhang, G., Wang, S., Peng, X., Ziqi, W., Mao, J., Wu, H., Jiang, X., & Wang, K. (2024). CaT-GNN: Enhancing Credit Card Fraud Detection via Causal Temporal Graph Neural Networks. arXiv preprint arXiv:2402.14708.
[32] Emmanuel, D. U., Ali, J. G., Yakubu, B., Shidawa, A. B., Job, G. K., & Lawal, M. A. (2023). Machine Learning-Based Intrusion Detection System for Cyber Attacks in Private and Public Organizations. International Journal, 12(5).
[33] Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. IEEE Access, 10, 16400-16407.
[34] Fakiha, B. (2023). Forensic Credit Card Fraud Detection Using Deep Neural Network. Journal of Southwest Jiaotong University, 58(1).
[35] Fatih, C. (2023). Comparing machine learning algorithms on credit card fraud problem Dublin Business School].
[36] Ferdous, F. S., Biswas, T., & Jony, A. I. (2024). Enhancing Cybersecurity: Machine Learning Approaches for Predicting DDoS Attack. Malaysian Journal of Science and Advanced Technology, 249-255.
[37] Gill, M. A., Quresh, M., Rasool, A., & Hassan, M. M. (2023). Detection of credit card fraud through machine learning in banking industry. Journal of Computing & Biomedical Informatics, 5(01), 273-282.
[38] Gongada, T. N., Agnihotri, A., Santosh, K., Ponnuswamy, V., Narendran, S., Sharma, T., & Baker El-Ebiary, Y. A. (2024). Leveraging Machine Learning for Enhanced Cyber Attack Detection and Defence in Big Data Management and Process Mining. International Journal of Advanced Computer Science & Applications, 15(2).
[39] Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., Khosravi, A., & Nahavandi, S. (2023). Uncertainty-aware credit card fraud detection using deep learning. Engineering Applications of Artificial Intelligence, 123, 106248.
[40] Hajek, P., Abedin, M. Z., & Sivarajah, U. (2023). Fraud detection in mobile payment systems using an XGBoost-based framework. Information Systems Frontiers, 25(5), 1985-2003.
[41] Hasan, M. R., Gazi, M. S., & Gurung, N. (2024). Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA. Journal of Computer Science and Technology Studies, 6(2), 01-12.
[42] Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of machine learning-based k-means clustering for financial fraud detection. Academic Journal of Science and Technology, 10(1), 33-39.
[43] Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 26, 101162.
[44] Jayaraj, R., Pushpalatha, A., Sangeetha, K., Kamaleshwar, T., Shree, S. U., & Damodaran, D. (2024). Intrusion detection based on phishing detection with machine learning. Measurement: Sensors, 31, 101003.
[45] Jovanovic, D., Antonijevic, M., Stankovic, M., Zivkovic, M., Tanaskovic, M., & Bacanin, N. (2022). Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. Mathematics, 10(13), 2272.
[46] Kaleel, A., & Polkowski, Z. (2023). Credit Card Fraud Detection and Identification using Machine Learning Techniques. Wasit Journal of Computer and Mathematics Science, 2(4), 159-165.
[47] Karthik, V., Mishra, A., & Reddy, U. S. (2022). Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model. Arabian Journal for Science and Engineering, 47(2), 1987-1997.
[48] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data and Cognitive Computing, 8(1), 6.
[49] Khan, S., Alourani, A., Mishra, B., Ali, A., & Kamal, M. (2022). Developing a credit card fraud detection model using machine learning approaches. International Journal of Advanced Computer Science and Applications, 13(3).
[50] Kumar, A. (2024). Cybersecurity Threat Detection using Machine Learning and Network Analysis. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 1(1), 124-131.
[51] Kumar, B. R. (2024). AI Based Credit Card Fraud Detection using Machine Learning Technique. 06(04).
[52] Kumar, S., Srija, K., Ramcharan, D., Jhansi, B., Bhavani, J., & Ganesh, L. (2024). Combatting Online Fraud: Advancing Fraud Detection in Internet Loans through Deep Learning Innovations. RES MILITARIS, 14(4), 372-380.
[53] Labu, M. R., & Ahammed, M. F. (2024). Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. Journal of Computer Science and Technology Studies, 6(1), 179-188.
[54] Lei, Y.-T., Ma, C.-Q., Ren, Y.-S., Chen, X.-Q., Narayan, S., & Huynh, A. N. Q. (2023). A distributed deep neural network model for credit card fraud detection. Finance Research Letters, 58, 104547.
[55] Maithili, K., Kumar, T. S., Subha, R., Murthy, P. S., Sharath, M., Gupta, K. G., Ravuri, P., Madhuri, T., & Verma, V. (2024). Development of an efficient machine learning algorithm for reliable credit card fraud identification and protection systems. MATEC Web of Conferences,
[56] Meduri, K. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. International Journal of Science and Research Archive, 11(2), 915-925.
[57] Minastireanu, E.-A., & Mesnita, G. (2019). An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection. Informatica Economica, 23(1).
[58] Ming, R., Abdelrahman, O., Innab, N., & Ibrahim, M. H. K. (2024). Enhancing fraud detection in auto insurance and credit card transactions: a novel approach integrating CNNs and machine learning algorithms. PeerJ Computer Science, 10, e2088.
[59] Mitchell, C. (2023). Identity Theft Prediction Model using Historical Data and Supervised Machine Learning: Design Science Research Study Colorado Technical University].
[60] Mohbey, K. K., Khan, M. Z., & Indian, A. (2022). Credit card fraud prediction using XGBoost: an ensemble learning approach. International Journal of Information Retrieval Research (IJIRR), 12(2), 1-17.
[61] Mohsen, O. R., Nassreddine, G., & Massoud, M. (2023). Credit Card Fraud Detector Based on Machine Learning Techniques. Journal of Computer Science and Technology Studies, 5(2), 16-30.
[62] Mrčela, L., & Kostanjčar, Z. (2024). Probabilistic Deep Learning Approach to Credit Card Fraud Detection. 2024 47th MIPRO ICT and Electronics Convention (MIPRO),
[63] Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. Cluster Computing, 25(6), 3819-3828.
[64] Nabi, F., & Zhou, X. (2024). Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security. Cyber Security and Applications, 100033.

[65] Nalluri, V., Chang, J.-R., Chen, L.-S., & Chen, J.-C. (2023). Building prediction models and discovering important factors of health insurance fraud using machine learning methods. Journal of Ambient Intelligence and Humanized Computing, 14(7), 9607-9619.
[66] Nicolini, G., & Leonelli, L. (2021). Financial frauds on payment cards: The role of financial literacy and financial education. INTERNATIONAL REVIEW OF FINANCIAL CONSUMERS.
[67] Noviandy, T. R., Idroes, G. M., Maulana, A., Hardi, I., Ringga, E. S., & Idroes, R. (2023). Credit card fraud detection for contemporary financial management using xgboost-driven machine learning and data augmentation techniques. Indatu Journal of Management and Accounting, 1(1), 29-35.
[68] O'Brien, S. (2021). The criminal act of committing insurance fraud: The challenges facing insurers when detecting and preventing insurance fraud Dublin Business School].
[69] Omer, N., Samak, A. H., Taloba, A. I., El-Aziz, A., & Rasha, M. (2024). Cybersecurity Threats Detection Using Optimized Machine Learning Frameworks. Computer Systems Science & Engineering, 48(1).
[70] Ortiz-Ruiz, E., Bermejo, J. R., Sicilia, J. A., & Bermejo, J. (2024). Machine Learning Techniques for Cyberattack Prevention in IoT Systems: A Comparative Perspective of Cybersecurity and Cyberdefense in Colombia. Electronics, 13(5), 824.
[71] Orunsolu, A. A., Sodiya, A. S., & Akinwale, A. (2022). A predictive model for phishing detection. Journal of King Saud University-Computer and Information Sciences, 34(2), 232-247.
[72] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. bmj, 372.
[73] Patel, K. (2023). Credit card analytics: a review of fraud detection and risk assessment techniques. International Journal of Computer Trends and Technology, 71(10), 69-79.
[74] Prasad, P. Y., Chowdary, A. S., Bavitha, C., Mounisha, E., & Reethika, C. (2023). A comparison study of fraud detection in usage of credit cards using machine learning. 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI),
[75] Priscilla, C. V., & Prabha, D. P. (2020). Credit card fraud detection: A systematic review. Intelligent Computing Paradigm and Cutting-edge Technologies: Proceedings of the First International Conference on Innovative Computing and Cutting-edge Technologies (ICICCT 2019), Istanbul, Turkey, October 30-31, 2019 1,
[76] Qaddoura, R., & Biltawi, M. M. (2022). Improving fraud detection in an imbalanced class distribution using different oversampling techniques. 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI),
[77] Qayoom, A., Khuhro, M. A., Kumar, K., Waqas, M., Saeed, U., ur Rehman, S., Wu, Y., & Wang, S. (2024). A novel approach for credit card fraud transaction detection using deep reinforcement learning scheme. PeerJ Computer Science, 10, e1998.
[78] Rangineni, S., & Marupaka, D. (2023). Analysis of data engineering for fraud detection using machine learning and artificial intelligence technologies. International Research Journal of Modernization in Engineering Technology and Science, 5(7), 2137-2146.
[79] Reddy, V. V. K., Reddy, R. V. K., Munaga, M. S. K., Karnam, B., Maddila, S. K., & Kolli, C. S. (2024). Deep learning-based credit card fraud detection in federated learning. Expert Systems with Applications, 124493.
[80] Roseline, J. F., Naidu, G., Pandi, V. S., alias Rajasree, S. A., & Mageswari, N. (2022). Autonomous credit card fraud detection using machine learning approach☆. Computers and Electrical Engineering, 102, 108132.
[81] Rtayli, N., & Enneya, N. (2023). Credit card fraud detection using predictive features and machine learning algorithms. International Journal of Internet Technology and Secured Transactions, 13(2), 159-176.
[82] Saddi, V. R., Boddu, S., Gnanapa, B., Jiwani, N., & Kiruthiga, T. (2024). Leveraging Big Data and AI for Predictive Analysis in Insurance Fraud Detection. 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS),
[83] Saeed, U. (2022). Visual similarity-based phishing detection using deep learning. Journal of Electronic Imaging, 31(5), 051607-051607.
[84] Saeed, V. A., & Abdulazeez, A. M. (2024). Credit Card Fraud Detection using KNN, Random Forest and Logistic Regression Algorithms: A Comparative Analysis. Indonesian Journal of Computer Science, 13(1).
[85] Saghir, W., & Kafteranis, D. (2022). The Applicable Law on Digital Fraud. In Finance, Law, and the Crisis of COVID-19: An Interdisciplinary Perspective (pp. 221-235). Springer.
[86] Saheed, Y. K., Baba, U. A., & Raji, M. A. (2022). Big data analytics for credit card fraud detection using supervised machine learning models. In Big data analytics in the insurance market (pp. 31-56). Emerald Publishing Limited.
[87] Sahithi, G. L., Roshmi, V., Sameera, Y. V., & Pradeepini, G. (2022). Credit card fraud detection using ensemble methods in machine learning. 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI).
[88] Sarker, A., Yasmin, M. A., Rahman, M. A., Rashid, M. H. O., & Roy, B. R. (2024). Credit Card Fraud Detection Using Machine Learning Techniques. Journal of Computer and Communications, 12(6), 1-11.
[89] Sharma, A., & Babbar, H. (2023). Machine Learning-Driven Detection and Prevention of Cryptocurrency Fraud. 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE),
[90] Shetty, V. R., & Malghan, R. L. (2023). Safeguarding against cyber threats: machine learning-based approaches for real-time fraud detection and prevention. Engineering Proceedings, 59(1), 111.
[91] Shome, N., Sarkar, D. D., Kashyap, R., & Lasker, R. H. (2024). Detection of Credit Card Fraud with Optimized Deep Neural Network in Balanced Data Condition. Computer Science, 25(2).
[92] Sinčák, J. (2023). Machine Learning Methods in Payment Card Fraud Detection.
[93] Singh, I., Aditya, N., Srivastava, P., Mittal, S., Mittal, T., & Surin, N. V. (2023). Credit Card Fraud Detection using Neural Embeddings and Radial Basis Network with a novel hybrid fruitfly-fireworks algorithm. 2023 3rd International Conference on Intelligent Technologies (CONIT),
[94] Sorour, S. E., AlBarrak, K. M., Abohany, A. A., & Abd El-Mageed, A. A. (2024). Credit card fraud detection using the brown bear optimization algorithm. Alexandria Engineering Journal, 104, 171-192.
[95] Tamal, M. A., Islam, M. K., Bhuiyan, T., Sattar, A., & Prince, N. U. (2024). Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. Frontiers in Computer Science, 6, 1428013.
[96] Tenis, A., & Santhosh, R. (2023). Modelling of an Adaptive Network Model for Phishing Website Detection Using Learning Approaches. Full Length Article, 12(2), 159-159-171.
[97] Udayakumar, R., Joshi, A., Boomiga, S., & Sugumar, R. (2023). Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification. Journal of Internet Services and Information Security, 13(3), 138-157.

[98] Unogwu, O. J., & Filali, Y. (2023). Fraud detection and identification in credit card based on machine learning techniques. Wasit Journal of Computer and Mathematics Science, 2(3), 16-22.
[99] Uyyala, P., & Yadav, D. C. (2023). The advanced proprietary AI/ML solution as Anti-fraudTensorlink4cheque (AFTL4C) for Cheque fraud detection. The International journal of analytical and experimental modal analysis, 15(4), 1914-1921.
[100] Valavan, M., & Rita, S. (2023). Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers. Computer Systems Science & Engineering, 45(1).
[101] Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online payment fraud: from anomaly detection to risk management. Financial Innovation, 9(1), 66.
[102] Xu, M., Fu, Y., & Tian, B. (2023). An ensemble fraud detection approach for online loans based on application usage patterns. Journal of Intelligent & Fuzzy Systems, 44(5), 7181-7194.
[103] Yılmaz, A. A. (2023). A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection. Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, 66(1), 82-94.
[104] Yu, C., Xu, Y., Cao, J., Zhang, Y., Jin, Y., & Zhu, M. (2024). Credit card fraud detection using advanced transformer model. arXiv preprint arXiv:2406.03733.
[105] Zahid, S. Z. S., Muhammad, H. M. U. H. H., Hafeez, U., Iqbal, M. J. I. M. J., Asif, A. A. A., Yaqoob, S. Y. S., & Mehboob, F. M. F. (2024). Credit Card Fraud Detection using Deep Learning and Machine Learning Algorithms. Journal of Innovative Computing and Emerging Technologies, 4(1).
[106] Zhao, C., Sun, X., Wu, M., & Kang, L. (2024). Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification. Finance Research Letters, 60, 104843.
[107] Zhu, K., Zhang, N., Ding, W., & Jiang, C. (2024). An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection. IEEE Transactions on Artificial Intelligence.

AUTHOR

Dr. Hashim is an assistant professor in the Cybersecurity Dept., EMU University - Jordan. His research interests include databases, big data, ontologies, network security, Data Science, and image encryption.