Journal of Big Data

SURVEY Open Access

A systematic review of AI-enhanced techniques in credit card fraud detection

Ibrahim Y. Hafez[1], Ahmed Y. Hafez[2], Ahmed Saleh[3], Amr A. Abd El-Mageed[4*] and Amr A. Abohany[3,5]

*Correspondence: amr.atef@commerce.sohag.edu.eg

[1] Department of Computer Science and Engineering, Faculty of Engineering, Egypt-Japan University of Science and Technology, New Borg El-Arab, Alexandria, Egypt
[2] Department of Electronics and Communication Engineering, Faculty of Engineering, Egypt-Japan University of Science and Technology, New Borg El-Arab, Alexandria, Egypt
[3] Faculty of Computer and Information, Damanhur University, Damanhur, Egypt
[4] Department of Information Systems, Sohag University, Sohag 82511, Egypt
[5] Faculty of Computers and Information, Kafr El-Sheikh University, Kafrelsheikh, Egypt

Abstract

The rapid increase of fraud attacks on banking systems, financial institutions, and even credit card holders demonstrate the high demand for enhanced fraud detection (FD) systems for these attacks. This paper provides a systematic review of enhanced techniques using Artificial Intelligence (AI), machine learning (ML), deep learning (DL), and meta-heuristic optimization (MHO) algorithms for credit card fraud detection (CCFD). Carefully selected recent research papers have been investigated to examine the effectiveness of these AI-integrated approaches in recognizing a wide range of fraud attacks. These AI techniques were evaluated and compared to discover the advantages and disadvantages of each one, leading to the exploration of existing limitations of ML or DL-enhanced models. Discovering the limitation is crucial for future work and research to increase the effectiveness and robustness of various AI models. The key finding from this study demonstrates the need for continuous development of AI models that could be alert to the latest fraudulent activities.

Keywords: Fraud attacks, Fraud detection (FD), Credit card fraud detection (CCFD), Machine learning (ML), Deep learning (DL), Meta-heuristic optimization (MHO), Cybersecurity

Introduction

The internet has grown astonishingly in the face of rapidly changing technological advances like big data, software-defined networking, and cloud computing. Nevertheless, serious cybersecurity risks are associated with these developments, which significantly impact essential infrastructure. Traditional safety techniques have found it challenging to keep up with the sophistication of new cyber-attacks since they rely on fixed safety mechanisms like intrusion prevention and fraud system detection [1]. DL has become a disruptive force that opens new opportunities for improved performance, data accessibility, and further optimization. It has not only revolutionized voice, image, and behavioral analytic applications in AI, but it has also brought revolutionary developments in robotics, speech recognition, and facial recognition. DL has been developed as a crucial tool in cybersecurity for malware monitoring and intrusion detection. Compared to previous ML applications, this represents a significant advancement [2]. While ML has demonstrated some potential, its dependence on human characteristic extraction has been verified to be problematic, particularly in cybersecurity. For instance,

manually producing malware features for ML-based recognition limits the effectiveness and reliability of attack identification to characteristics and ignores unknown behaviors. As a result, feature extraction and recognition accuracy determine how good ML is [3]. Because DL can find complex, nonlinear relationships in data, it gives Cyber Defense2 a strategic advantage by making previously unidentified fraud attacks visible. Significantly, DL has advanced measures to stop Advanced Persistent Threat (APT) attacks, even identifying the fine-grained, sophisticated characteristics employed in the most fraudulent tactics [4].

In order to create advanced intrusion detection systems, ML is used in the face of automated behavior analysis by extracting essential features from network packets. Essentially, ML is about allowing computers to learn and adapt independently without human help [5]. In the modern era, cybersecurity aims to reduce the likelihood of threats and unlawful access by utilizing a set of methods, regulations, and standards that uphold data privacy and security. Systems with the ability to recognize essential indicators of possible breaches are desperately needed as the complexity and frequency of attacks are growing. DL is an essential advancement in cybersecurity techniques since, despite its complications, it can generate accurate results after being educated appropriately [5]. This paper targets to study various applications of ML, DL, and MHO, focusing on credit card fraud (CCF) attacks by discovering their effectiveness and accuracy and addressing future work for further research and development of fraud detection (FD) systems.

Motivation

ML, DL, and MHO algorithms have opened a fresh path in FD, which provide highly sophisticated features for real-time analysis of massive transaction data. These technologies can completely change how financial organizations secure individuals and their investments. Despite all of the advancements in technology, there is still a lack of detailed reviews of the most recent developments, comparisons of their efficacy, and identification of the obstacles that still need to be addressed in the literature.

This paper aims to attempt to address this lack by presenting a reasonably thorough synthesis of recent advancements in this subject and offering insights that might guide future investigation and application. As a result, it supports and encourages ongoing efforts to develop more robust and adaptable FD systems, which will ultimately improve the security of online financial transactions.

Main contribution

The paper's primary contribution is a comprehensive collection of recent studies on CCF attacks and the systems that detect them. It presents existing issues and unfulfilled research needs, giving academics a clear picture and a strong starting point for more investigation into the application of AI to fraud threat detection and mitigation. The research's contributions can be summarized in the following topics:

- An overview of the effectiveness of ML, DL, and MHO methods for identifying CCF attacks, categorization, and analytical approaches.

- An analysis and critical assessment of more than thirty scholarly articles published between 2019 and 2024 concentrated on applying fundamental AI methods and utilizing cybersecurity in CCFD.
- Evaluation of the articles based on a number of factors, including the methodology, datasets, AI techniques applied, data sorting strategies, methodological comparisons, and performance metrics.
- Assessment of the most recently used datasets as well as free access to CCFD datasets
- Crucial components of the investigations are arranged into comparative tables that provide a brief overview for comprehending the various strategies and outcomes.
- A summary that highlights the challenges that today's AI techniques in detecting CCF face and offers potential future solutions.

Paper structure

The study offers a systematic investigation of AI techniques in fraud attack detection and is structured into six main sections. In Sect. "Introduction", the scientific resources and inspirations have been presented. This is followed by Sect. "Background", which covers the history of the study and outlines its primary subjects. The relevant literature has been reviewed in Sect. "Literature review". A brief description of the research technique has been provided in Sect. "Methodology". The findings have been examined and talk about the causes in Sect. "Results and discussion". Lastly, a summary of the entire content is provided in Sect. "Conclusion".

Background

The development of computer networks has altered society and increased the frequency and sophistication of cyberattacks. Disruptive activities directed toward computer networks, systems, or data are known as cyberattacks. They often follow a coordinated set of steps to accomplish their objectives and are well-organized and well-planned [3]. Insider threats, which constitute a significant and expanding part of these attacks, are characterized as intentionally causing harm, illegal entrance, or interruptions of services that result in significant theft of data or economic loss and frequently have long-term results [6]. These attacks are typically carried out by criminal or disgruntled employees who take advantage of their authorized entry to obtain information or cause damage. Unintentionally installed intrusive applications on devices may also pose a concern since they provide access to and misuse of private information.

Techniques for robust and sophisticated behavioral fraud detection are being enhanced to proactively detect and mitigate malicious behaviors at the application and staff levels in order to counter these attacks [6]. Cyberattacks may come in a wide range and symbolize different kinds of threats associated with the digital realm. Figure 1 provides insights into numerous significant categories of these attacks. The complication and diversity of cyberattacks are highlighted by this data, which also illuminates various types of threats that individuals and organizations might experience in today's linked world [3].

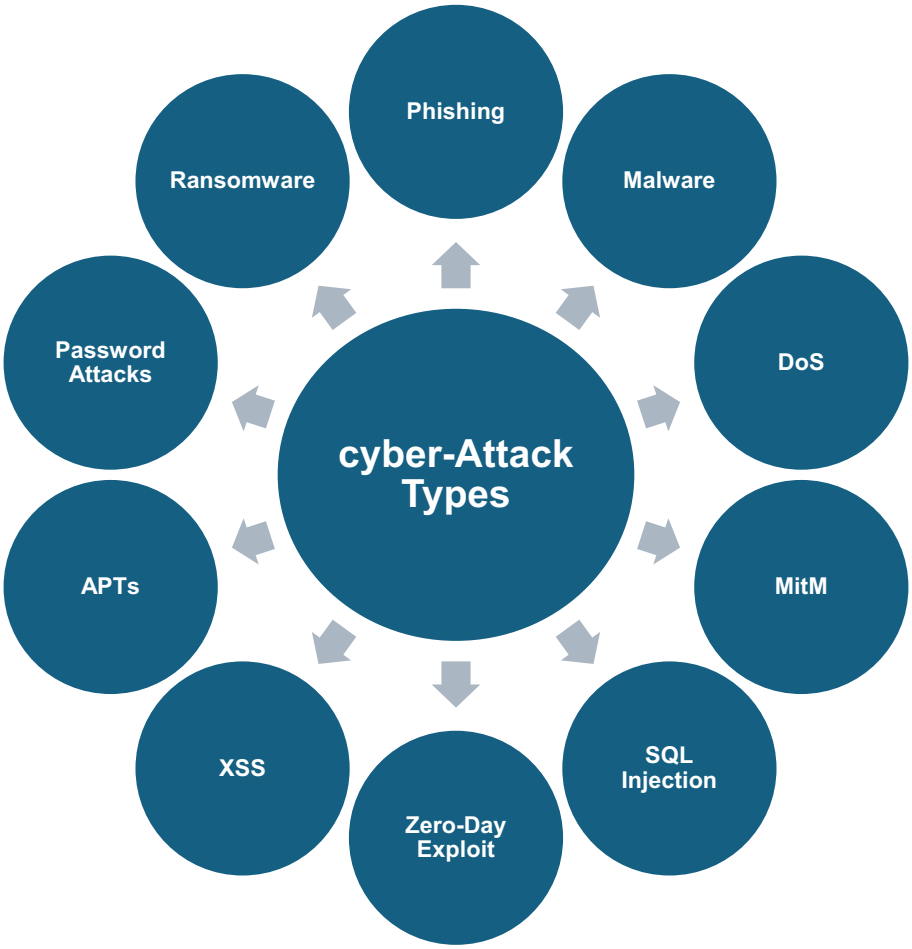

Fig. 1 Cyber-attack types

In this study, we will concentrate on CCF attacks. The financial damages made due to fraudulent schemes underscore the critical requirement for efficient cybersecurity techniques. It should be noted that numerous cyberattack types, including phishing, skimming, SQL injection, and others, are linked to CCF. Securing sensitive data and maintaining the functionality of digital services are essential. Because fraud risks are constantly evolving, it's critical to stay aware and keep spending money on cutting-edge security solutions. In order to stay ahead of cyber risks, one must actively adjust to new attacks, utilize optimal approaches, and leverage technological advances to protect against the attackers' varied [7, 8].

The cybersecurity community has put a lot of emphasis on fraud identification as a critical tactic against the expanding attacks. That method includes thorough monitoring of system safety, network activity, and usage patterns in order to detect and prevent unwanted access or harm in advance. In this context, AI, ML, and DL demonstrate fascinating means of boosting cybersecurity. Because AI can adapt quickly and manage big data sets, it's an excellent approach to detecting and mitigating advanced cyber threats. AI-based applications could identify various types of

attacks, such as malware, phishing attempts, and other harmful activity, by examining patterns and learning from past experiences [9].

Artificial Intelligence

Pioneers like John McCarthy defined AI as the science and engineering of creating intelligent machines in 1956 [10]. AI, which focuses on utilizing sophisticated mathematical algorithms to mimic human cognitive processes, has developed into a vital component of computer science over time. This multidisciplinary field adopts systems that could learn, evaluate, and generate judgments depending on the information they process by combining aspects from many domains. Furthermore, it includes the imitation of human cognition and behavior in robots, which are classified as thinking and acting in human and rational ways, respectively [11]. Applications of AI range from straightforward jobs to intricate problem-solving in fields like cybersecurity, where it tackles sophisticated online threats. With the goal of augmenting, and autonomous intelligence to automate jobs and improve human capabilities, this game-changing technology keeps pushing the boundaries of what machines can do.

The application of AI in cybersecurity is becoming more critical because of its ability to quickly analyze large volumes of data, spot trends, and efficiently identify possible risks. Traditional security methods frequently lack the speed and sophistication required to handle new attacks, particularly zero-day threats, in a digital age marked by constantly changing cyber threats [12]. The capacity of AI to learn from data facilitates the creation of systems that can adjust to novel, unidentified attacks, improving the security of information infrastructure against a wide range of threats. Better decision-making skills, more effective network intrusion detection, and better impact management are some of the advantages of integrating AI into cybersecurity. Technological advancements have made it possible to detect and respond to threats in real-time while also significantly reducing the number of false positives, which is a problem that affects older cyber defense strategies. Moreover, AI's predictive analytics provides proactive security as opposed to reactive security by anticipating such weaknesses before they are exploited. Essentially, AI provides sophisticated analytical capabilities to cybersecurity, making it a vital partner in the fight against cybercrime [13]. AI technologies include a number of methods that are helpful in cybersecurity, including:

- ML: Algorithms that let computers learn from data without the need for explicit programming, leading to better risk identification and categorization [14].
- DL: State-of-the-art neural networks that can handle massive volumes of data, learn from mistakes, and reproduce complex patterns in the way the human brain works [4].

Because these AI techniques enable real-time monitoring, automatic reactions, and continual learning to adjust to new risks or threats, they offer strong defenses against cyberattacks.

Machine learning (ML)

The purpose of this section is to provide a brief review of ML approaches, categorizations, and structures. ML is an area that enables computers to handle issues and comprehend them without the need for explicit programming. The learning technique includes various ML techniques, which are distinct significantly and classify them based on their tasks or the complexity of their operations [15].

ML techniques are generally classified into basic and depth learning, as shown in Fig. 2. The basic ML are divided into supervised, unsupervised, reinforcement, semi-supervised, active, and ensemble learning. A collection of labeled pairs of inputs and outputs that direct the algorithm during development is known as supervised learning. Analyzing the data entails creating a function that maps from inputs to outputs and tasks involving classification and regression are typical implementations of supervised learning method.

On the other hand, unsupervised learning is a method looks for structures or trends in the information based on its intrinsic properties rather than using labeled data for learning. It concentrates on tasks such as dimensionality reduction, clustering, and association rule learning without predefined labels or outcomes. Threats in unsupervised learning frequently target specific language models. Reinforcement learning functions by utilizing methods of trial and error learning in conjunction with an outside setting. With regard to acquired experiences, it creates estimates about upcoming outcomes—notably, in this educational paradigm—without recorded attacks on confidentiality.

Semi-supervised learning is an approach, which combines aspects of supervised and unsupervised learning, trains models using a combination of labeled and unlabeled data. The unlabeled data improves comprehension, and the labeled component is used to refine challenges. It is frequently used in problems involving regression and classification. In order to minimize the requirement for large labeled datasets, active learning algorithms deliberately choose training data, which optimizes the time as well as the expense associated with obtaining labeled training data. In ensemble learning, an effective classifier that bases its judgments on the combined expectations

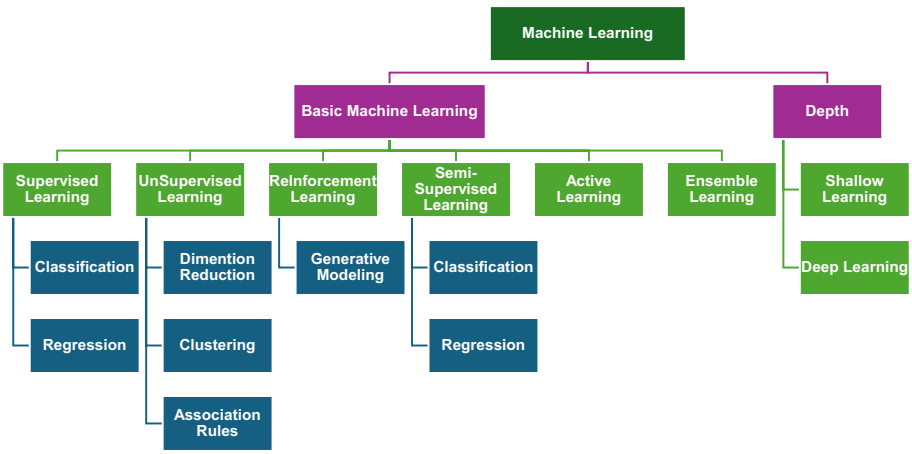

Fig. 2 Classification of ML techniques [15]

of individual models is created by combining several weak classifiers together. Methods like bagging and boosting are examples of group learning procedures [14].

Various ML algorithms have shown a vital role for developing efficient models for detecting cyberattaks and fraud. For example, Linear Classifiers (LC) which are linear algorithms, use decision boundaries to separate input vectors into classes. This classification aims to gather similar features together into categories [16]. In classification issues, Logistic Regression (LR) approach is used to predict the outcome for a categorical dependent variable. It is specifically designed for tasks that require the output to be a distinct or classified value, such as binary classification [17]. Gaussian Naive Bayes (GNB) is a Gaussian distribution-based statistical categorization method. It operates under the assumption that each factor influences the possibility of the result separately, summing the likelihoods to determine the most likely category [18]. Additionally, Support Vector Machine (SVM) is a technique that operates by identifying a separating hyperplane between various classes by converting the data into a higher-dimensional space. Even in cases when the data are not linearly separable in the original space, this technique works well [19]. The technique of Decision Tree (DT) creates a tree-structured model. It divides information according to qualities, attempting to predict a target variable using straightforward decision rules by representing options as branches and outcomes as leaf nodes [20].

Deep learning (DL)

Within the discipline of ML, DL is a specialized domain that focuses on representation learning through multilayer transformations, improving detection and prediction accuracy. DL-enhanced defensive mechanisms are being employed more frequently in cybersecurity to identify cyber threats automatically. These systems are constantly changing and becoming more effective over time [17]. Depending on the computational layers, the input layer, hidden layer or levels, and output layer make up the fundamental structure of DL. Many prediction models built on artificial neural networks (ANNs), which are made up of interconnected networks of neurons that communicate with one another. Deep neural networks (DNNs) are distinguished from more basic single-hidden-layer neural networks by their significant depth, which is characterized by multiple hidden layers that enable complex pattern recognition. As demonstrated in Fig. 3, a DNN typically consists of an input layer, multiple hidden layers, and an output layer, with neurons producing nonlinear responses in each layer [4]. These architectures have a wide range of uses in cybersecurity, from creating sophisticated defense plans and intrusion detection systems to identifying network deviations and false data injection.

There are many DL models utilized in the filed of fraud attacks detection and each one has its advantages and existed limitations. For example, Convolutional Neural Networks (CNNs) are designed to efficiently process multi-array data structures, such as text or pictures, by utilizing standard weights and local connections. Convolutional and pooling layers are frequently included in CNNs, which result in wholly connected layers. CNNs are utilized in cybersecurity for tasks like fraud identification and user verification. Learning sequential data patterns is a strong suit for Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks, which incorporate memory elements to manage temporal relationships. By employing cell memory units with gate

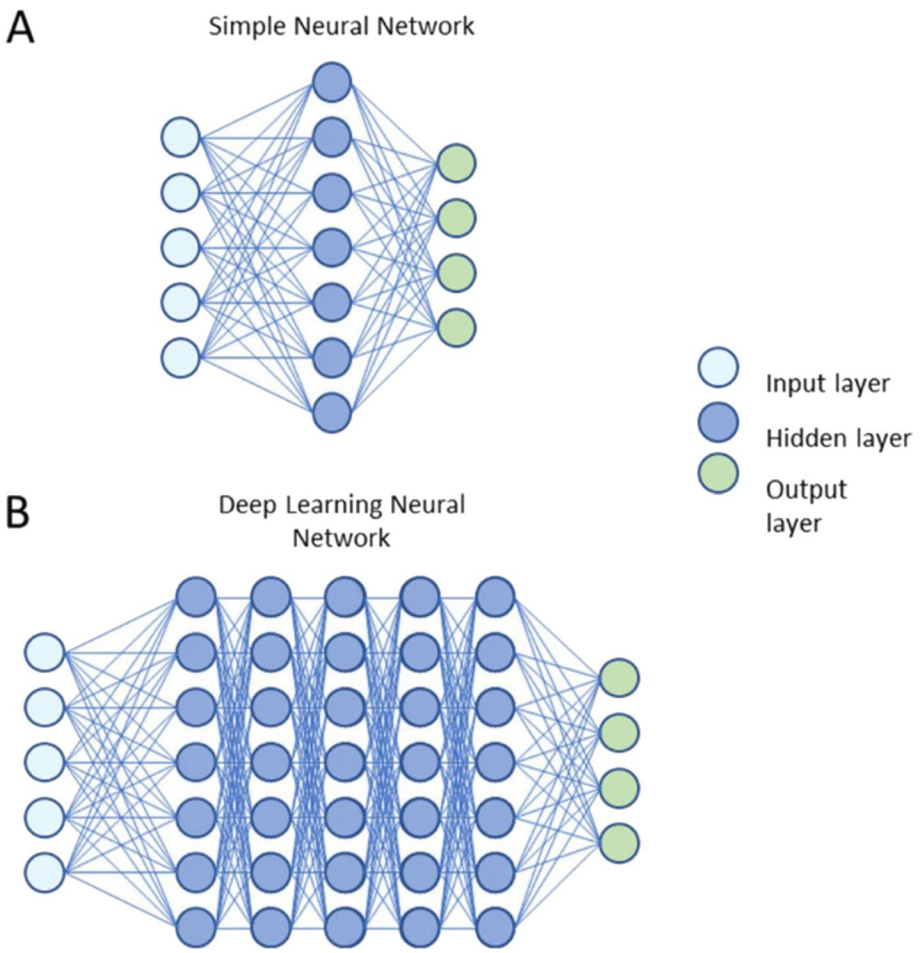

Fig. 3 Neural network vs deep neural network [21]

mechanisms, LSTMs solve the vanishing gradient issue with RNNs, which makes them suitable for evaluating dependent on time input. LSTM is a type of specialized RNN that is employed in sequence prediction algorithms, including time series evaluation and speech recognition. It solves the problem of diminishing gradients with conventional RNNs by incorporating three entry points: data input, forget, and output, which regulate the data transfer. Although LSTMs work well for forecasting time series and sorting, they are not appropriate for nonsequential information and need a lot of preparation.

Additionally, Feedforward Neural Networks (FNNs) process information in one path across hidden layers, moving from intake to result layers. They are not appropriate for sequential information, but they are easy and efficient for jobs like voice and picture recognition. To handle dependency over time and minimize the disappearing gradient issue, Gated Recurrent Units (GRU) are RNNs with upgraded and reorganized gates. Their proficiency lies in speech identification, language modeling, and time series estimation. Variational Autoencoders (VAE) encode data into a space of variables using probabilistic techniques to produce fresh, comparable data instances. They're employed in data enhancement, discovering anomalies, and image production. Other DL models such as Graph Neural Networks (GNN) which use message-passing methods to

aggregate and update node attributes in order to handle graph-structured input. They work well in a variety of areas for graph categorization, link estimation, and node characterization. Autoencoders (AEs) use the encoder and decoder elements for feature training and decreasing dimensionality in order to recreate their input at the output. AEs are helpful for problems like junk mail and the detection of intrusions, and they are used in unsupervised learning [15].

In summary, because of their capability to recognise intricate relationships and trends in transactions, DL models such as CNNs, RNNs and LSTM networks provide unique benefits for CCFD. While RNNs and LSTMs are excellent at detecting temporal correlations and are therefore suited for sequencing transaction evaluation, CNNs are especially efficient at collecting spatial information. The detection systems can greatly improve efficiency and lower false positives by utilising these models. As the technology develops, these models' effectiveness will be further enhanced by hyperparameter adjusting and integration with MHO approaches, solidifying DL's position as a key component in the battle against CCF.

MHO algorithm

The primary objective of MHO algorithms is to explore and take advantage of the search space in order to find optimal or nearly optimal solutions in challenging circumstances. They effectively avoid local optima and are derivative-free and adaptable. These algorithms, in contrast to gradient-based techniques, do not require derivative computations and instead begin their optimization process with one or more randomly generated solutions. With the use of MHOs, potential search spaces are explored, and local searches of promising locations are conducted in a balanced manner [22].

Sophisticated global optimization techniques called MHO algorithms are based on naturalistic approaches. These approaches have been proven successful for many years; they are based on the social and swarm characteristics found in many species, including fish, birds, ants, and other animals. The ability of these creatures to solve complicated problems with efficiency and collective intelligence opened the door for the creation of optimization algorithms. These algorithms, which use the concepts of collective behavior to provide ideal solutions, have shown significant success in a variety of real-world optimization tasks [23].

MHO techniques are mainly categorized into four types, which are evolution, swarm intelligence, physics, and human behavior-based algorithms. As demonstrated in Table 1, this classification is predicated on how they behave and where they find inspiration, which ranges from physics principles and human activities to natural processes and animal behavior.

There are several benefits to combining learning models and MHO algorithms for cyberattack detection [16]. By expanding the search space examined during model training, MHO algorithms enhance learning and might potentially reveal superior solutions that standard approaches would miss. MHO algorithms make them essential for boosting the speed and accuracy of various detection learning applications. Additionally, they are beneficial for cybersecurity because attack tactics and the environment are constantly changing. Additionally, by facilitating more dynamic model adaptation to novel or developing cyber threat types, models are better able

Table 1 Popular MHO classifications [24]

Evolution-based Algorithm
1. Genetic Algorithm: It uses crossovers, mutations, and reproduction—fundamental aspects of biological evolution—to generate responses 2. Differential Evolution: It focuse on population-based mutations, crossovers, and selections to produce imaginative vectors equivalent to the GA
Swarm Intelligence-based Algorithm
1. Particle Swarm Optimization: Motivated by the group-based behaviors of fish schools and migrating birds, the swarm optimizes outcomes by pooling its shared knowledge 2. Butterfly Optimization Algorithm: It simulates the way butterflies use scent emissions to find feed or partners; this is done for optimization purposes
Human-related Algorithm
1. Teaching–Learning-Based Optimization: It simulates the procedure of instruction and comprehension in a classroom setting, where the most effective answers are refined continuously via the stages of the instructor and the student 2. Harmony Search: Motivated by the harmonic discovery procedure in musical instruments with an emphasis on randomization, tone correction, and memory concern
Physics-based Algorithm
1. Gravitational Search Algorithm: It uses massed particles as searching tools to identify the best options; the concept depends on Newton's principles of gravity

to generalize across various datasets and scenarios [17]. The benefits of Cyber Attack Detection employing MHO Algorithms can be summarized in the following points [16]:

- *Optimization*: MHO algorithms are superior at identifying the best answers to complicated challenges that would otherwise be too difficult for traditional techniques to tackle.
- *Automation*: These algorithms reduce the need for human interaction by automating the changing of detection parameters, which speeds up and improves the accuracy of the detection process.
- *Speed*: They frequently arrive at practical solutions more quickly, which is crucial in cybersecurity environments where threats need to be promptly recognized and eliminated.

In order to conclude the background section, we've dived into the complex realm of cybersecurity, emphasizing the dangers of cyberattacks and the pressing need for reliable detection systems. One incredibly successful method has been demonstrated to be the integration of MHO algorithms with cutting-edge technologies like AI, ML, and DL. This effective combination dramatically enhances the capacity to recognize and address cyber threats. An introduction of each technological component has been provided.

Literature review

The exponential rise of financial services and online sales in the twenty-first century has made CCF a severe threat. Because CCF can result in significant financial losses, professionals and scholars must create efficient FD systems. Because traditional rule-based systems can't evolve to keep up with the growing nature of criminal activity, they are no longer appropriate. As a result, there is increasing demand for using DL, ML, and MHO techniques to identify fraud more successfully. This literature study

dives into the diverse methodologies and strategies utilized in detecting cases of CCF, with a particular focus on their unity with cybersecurity protocols and AI.

Hussain et al. [25] demonstrated the use of RF, DT, and SVM algorithms to enhance the accuracy of FD. Their paper focuses intensely on utilizing the RF technique, which is a classification process for monitoring datasets and increasing the efficiency of the output data. All the algorithms used are tested based on a set of parameters such as accuracy, sensitivity, and precision. Sulaiman et al. [26] represented various ML algorithms for CCFD and secure card holders' data. In order to increase the accuracy of FD and enhance privacy, their research suggests an effective hybrid model based on ML techniques, especially ANN. Similarly, Aziz and Ghous [27] investigated a range of DM approaches specifically designed to identify CCF, concentrating on several ML methodologies like RF, SVM, HM, DT, and DL. Based on previous actions, these techniques were used to determine typical customer behavior patterns. Their analysis of ML methods revealed significant discrepancies between various studies and recommended directions for more investigation.

Ali et al. [28] categorized financial frauds into distinct types, such as financial statement fraud and CCF, utilizing popular ML methods for FD, such as SVM and ANN. They also divide credit card fraudulent activities into two types: offline and online fraud. Their review outlined the primary problems, weak points, and restrictions in the field of financial fraud detection and offered ideas for potential future work. A CCFD model was offered by Singh et al. [29], which integrates an MHO algorithm prompted by the bio-inspired firefly with two successive layers of an SVM. Using the firefly algorithm and the feature section methodology, the selected set of features was optimized in the first level, and the SVM classifier was used in the second level to create the training model for identifying incidents of CCF. With an accuracy of 85.65%, the model successfully classified 591 transactions. Behera et al. [30] proposed a FUZZGY hybrid model based on FL that categorized fraudulent and non-fraudulent transactions with reduced false positives. The technique utilized the ANN model and fuzzy c-means clustering. When the model was tested using synthetic data, the outcomes demonstrated that the integration of learning processes and clustering algorithms reduces the number of false positives.

Nguyen et al. [31] proposed a DL technique that detects CCF on European, Small, and Tall cards using different economic datasets. The technique relies on convolutional neural networks and LSTM. Using sampling strategies to address the problem of class imbalance, the research found that performance improved on samples that were already available but dramatically decreased on newly uncovered data. Based on research findings demonstrating that the recommended DL techniques outperform traditional ML models inCCFD, the suggested approaches have practical applications in identifying CCF. After comparing all of the methods, the LSTM with 50 blocks came out on top with an F1 score of 84.85%. For the purpose of developing balanced datasets for DL-based detection model training, Misra et al. [32] and Schlör et al. [33] employed under-sampling strategies. Under-sampling's potential to remove valuable data instances from the training set is a noteworthy drawback that could negatively impact the effectiveness of detection. On the contrary, dynamic models with different combination elements have been developed through the use of isolation techniques to estimate the data distribution.

Buschjäger et al. [34] give evidence of the successful application of this detection of outliers method in FD. However, there is an apparent lack of information in the literature about an in-depth evaluation of the most recent ML methods that employ undersampling to solve class imbalance concerns. Unrealized potential exists in hybrid semi-supervised approaches that integrate supervised learning with unsupervised outlier detection. Furthermore, the financial cost of these detections has been overlooked in favor of typical performance indicators when evaluating the effectiveness of detecting fraud in mobile payment applications. Using K-means and GA algorithms, Benchaji et al. [35] provide a novel approach to FD in credit card transactions, addressing the problem of the traditional methods in finding minority class items in imbalanced datasets. To acquire a freshly trained dataset, the researchers first used the K-means approach to categorize and group the minority cases. Next, they utilized the GA technique for each category to generate new instances. Furthermore, in order to address the issue of identifying fraudulent credit card transactions, Özçelik et al. [36] also employed the GA method as a MHO. Using transactional data from the actual world, the investigation was applied to a real-life project.

A key finding of the thorough examination of the body of literature is that FD is changing quickly due to the ever-changing strategies used by fraudsters, particularly in the context of credit card transactions. One crucial turning point in the fight against financial fraud is the move away from standard statistical techniques and towards more complex strategies like ML and multilevel hypothesis testing. These developments are not just little steps forward; they are critical in tackling the ongoing problem of unbalanced data, which seriously compromises the efficiency of detection systems. As a result, the field of FD is about to enter a new chapter in which the application of complex techniques could change the parameters for privacy in financial transactions conducted via the Internet. Continuous innovation in this field is essential, as it holds the potential to improve accuracy and strengthen the ability of economic systems to resist fraud attacks.

Methodology

Many approaches have been put forth to identify fraud attacks. A research strategy has been created using a systematic literature review methodology to investigate these issues methodically, as shown in Fig. 4. This procedure involves selecting studies, creating research questions, determining the research topic, and extracting data. More precise and thorough data analysis can be provided by applying qualitative and quantitative techniques in a mixed-methods approach [37].

Identify research topic

A range of studies have been methodically arranged in our research to offer a thorough but targeted analysis of AI-driven cybersecurity detection methods. Our primary goal in this broad area was to present the most significant and creative contributions. Reference to recent developments, methodological precision, a variety of techniques (ML, DL, and MHO), and the application of modern datasets were among the selection criteria. By doing this, we want to maintain the manageability of our review and offer insightful information without becoming excessively complex. By adopting this approach, we were able to examine these techniques' performance, drawbacks, and potential for

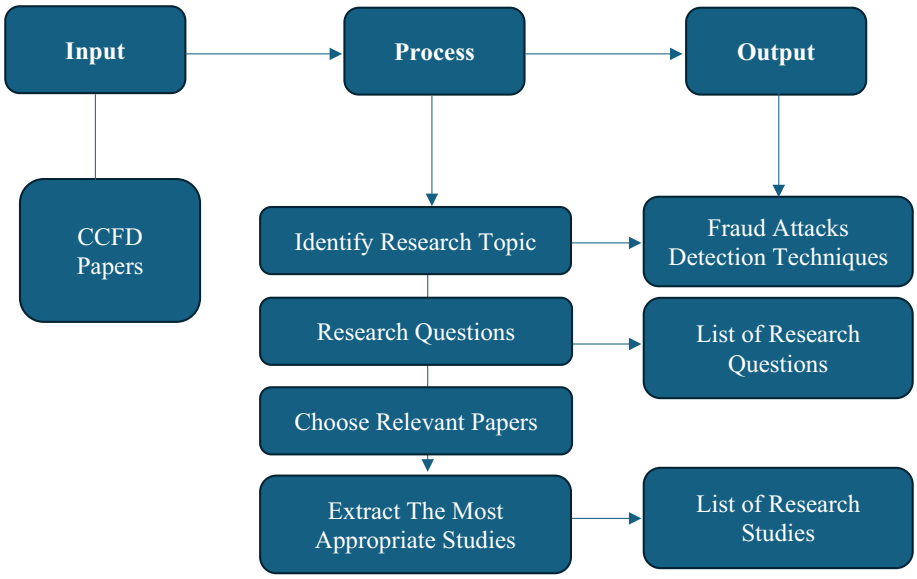

Fig. 4 Systematic literature review methodology

improvement in greater detail, which helped us to draw a clearer picture of where AI is headed in cybersecurity today and in the future. Thousands of contributions have been made; however, our selection process concentrated on those that offer noteworthy breakthroughs and valuable applications for identifying CCF attacks.

Our objective search approach focused on important review articles about fraud attack detection in order to collect a wide variety of studies. "*Fraud attack detection*" was our primary search keyword, which allowed us to find relevant articles in a thorough and well-planned search. Three research databases—Google Scholar, Scopus, and Web of Science—were evaluated before we began our review. The reason we chose Scopus is that in contrast to Google Scholar, which includes some non-peer-examined publications, such as technical papers, it covers a narrower range of publications from famous publishers such as ACM, Springer, and IEEE. The most recent techniques for detecting CCF attacks that have been released between 2019 and 2024 are our primary concentration. A total of 157,000 articles were published on Google Scholar, 17,000 of which were published between 2019 and 2024, according to our findings. Out of the 984 publications listed on Scopus, 621 were published during this period. About 600 publications were available on the Web of Science, 300 of which were published between 2019 and 2024.

Research Questions (RQs)

In order to direct our investigation, precise Research Questions (RQs) have been developed and concepts to analyze research papers. In order to better comprehend how these approaches are created and used, we first looked at the many kinds of procedures that are employed. The evaluation of these techniques was then looked at, along with an introduction to their difficulties, the datasets that are employed, and lastly, the suggested direction for future research. The RQs that this study aims to answer are as follows:

RQ1: Which ML, DL, and MHO models are used and applied to identify CCF attacks?

RQ2: What are the Big Data techniques utilized for CCFD in real time, and what are their limitations and proposed solutions?

RQ3: Which datasets are most frequently used to detect CCF attacks?

RQ4: What are the drawbacks of employing ML, DL, and MHO models in CCFD?

RQ5: What future directions are recommended for ML, DL, and MHO models in detecting CCF attacks?

Choose suitable papers

It was required to address a search string after choosing the digital databases in order to carry out a comprehensive search and choose the critical research. There were four phases involved in defining the search strategy:

1. Finding the appropriate results by using the previously established RQs.
2. Determining synonyms and alternate spellings for each significant word.
3. Confirming that the papers' keywords, abstracts, and titles contain search terms.
4. Using Boolean operators like "AND" and "OR" to create the search string effectively.

After applying the previously mentioned steps, the following search string was obtained: ("Credit Card Fraud Detection" OR "CCFD") AND ("Detection") AND ("Fraud Attacks" OR "Cyberattack" OR "Cyber Threats" OR "Cyber Attacks" OR "Cybersecurity") AND ("Meta-heuristic Technique" OR "Meta-heuristic" OR "Optimization Algorithms") AND ("Artificial Intelligence" OR "AI") AND ("Machine Learning" OR "ML") AND ("Deep Learning" OR "DL"). All published papers were put together in an effort to cover as much area as possible in the relevant literature between 2019 and 2024 using the search string method. As indicated in Table 2, we developed inclusion and exclusion criteria for use with the primary studies selection process.

Extract the most appropriate studies

The studies retrieved from the Scopus database have been filtered using the criteria we had developed, as shown in Fig. 5. Using our selected search keyword, 628 studies were initially collected. For the primary screening step, 109 studies were left after the other studies were eliminated according to the keywords, titles, and abstracts. It is also

Table 2 Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
■ Studies related to credit card fraud detection (CCFD) ■ Studies employing Artificial Intelligence, Machine Learning, Deep Learning, and Metaheuristic techniques ■ Peer-reviewed research published in scientific journals or conferences	■ Papers that are less than six pages since they usually lack a suitable research content ■ Research concentrating on fraud detection methods not related to Machine Learning, Deep Learning, or Meta-heuristics ■ Studies that lack results, surveys, and statistical analysis ■ Articles for which the complete text is not available

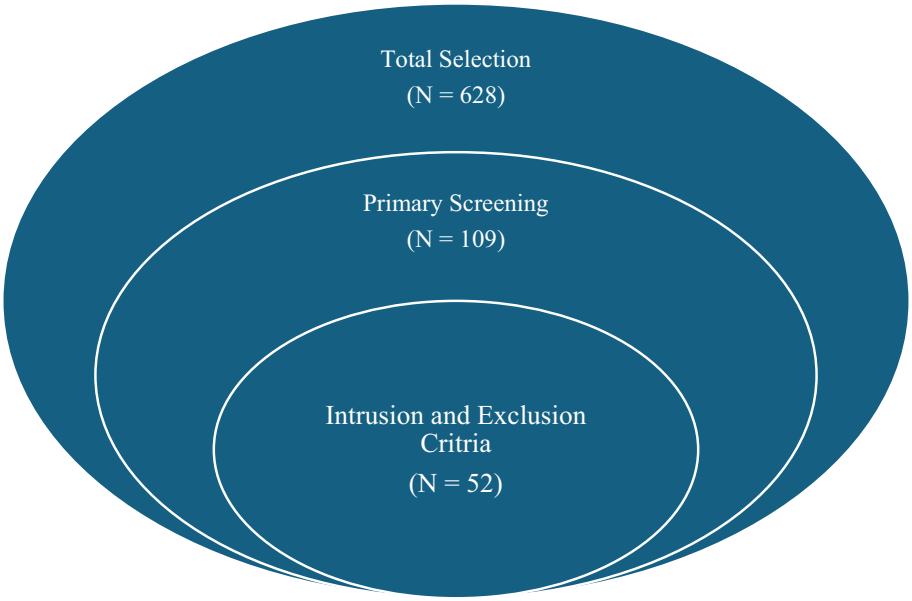

Fig. 5 Criteria of selecting studies

possible to reduce these studies to 52 studies by properly implementing the inclusion and exclusion criteria.

Vital information was extracted from each document, categorized and examined. The year of publication, authors, citation measure, area of study, model, measurement parameters, and dataset were among the details from the paper that were included in this. Each research was also examined in light of the kind of learning strategy that was employed. In order to organize this data, we first looked over each paper's title, abstract, and introduction, which usually included all the relevant information. We didn't look up further information in the entire text until we required it. Papers have been selected based on their content, length, and level of quality in order to create a collection that would be useful for investigation and evaluation.

Results and discussion

This section presents the extensive investigation and evaluation of the research results, with an emphasis on the efficiency of CCFD techniques. Our evaluation thoroughly addresses the RQs stated in Subsect. "Research Questions (RQs)", offering comprehensive responses that effectively advance the field while also enhancing comprehension. The results are provided in a format that other scholars might develop further, providing an excellent basis for future studies and innovations.

RQ1: Which ML, DL, and MHO models are used and applied to identify CCF attacks?

- ML Models

  To address the research topic of using ML to detect CCF, we conducted an extensive review of the literature. This required a methodical collection of current research articles that addressed ML techniques in the context of cybersecurity. Notably,

Table 3 Recent papers of ML models in CCFD

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[42]	2019	LR, NB, RF, and MLP	Models' accuracy (%): LR: 97.46, NB: 99.23, RF: 99.96, MLP: 99.93	Kaggle CCF Dataset	• High accuracy with improvement of FD rate	• Adaptation complexity to different domains	Window 10 Operating System, Spyder environment	Improve the FD rate
[43]	2019	LOF, SVM, LR, DT, and RF	The best accuracy of 0.9998 for RF	European Credit Card Dataset	• Handling imbalanced datasets	• High processing time and computational intensity	Python, Jupiter Notebook	Increase FD rate of credit card transactions
[44]	2019	LR, NB, LR, and SVM	Accuracies: 74%, 83%, 72%, and 91%	Financial Institution Dataset	• Higher performance and accuracy	• Computationally intensive for large datasets • Requirement of hardware specifications	NA	Concentration on location-based frauds and prediction levels
[45]	2020	LR, NB, and KNN	Highest accuracy for LR of 0.959	Mastercard European Transaction Dataset from Kaggle	• Optimal classification performance High accuracy	• Imbalanced datasets • High dimensional data leads to high computational expenses	Python	Improve FD systems
[46]	2020	Supervised, Enemble, Pipeling Learning Algorithms	Best Accuracy for Pipeling Learning: 99.9999%	ULB ML Group Dataset	• High accuracy of FD	• Process complexity • High usage of memory for the ensemble techniques	Python—Scikit-learn library	Develop hybrid models and real-time processing
[47]	2022	KNN, NB, LR, and SVM	The best accuracy of 99.94% for the SVM model	Kaggle European Credit Card Dataset	• High security and accuracy of FD	• Difficulty with big data • Time delays due to SVM processing	Weka and R program	Increase the security of the transaction process
[48]	2022	RF, LR and Gradient Boosting (GB)	Accuracies: 80%, 70%, above 90%	Data colledted from Lending Club website	• Maximum efficiency obtained with ensemble learning	• Large data demand • A large capacity memory and storage requirement	NA	The exploration of neural networks and DL incorporated with MLs
[38]	2023	DT, LR, XGBoost, ANN	Best result is for XGBoost: F1-Score: 0.856, Precision: 0.913, Recall: 0.805, Accuracy: 0.99	Credit Card Fraud Detection Dataset	• High accuracy score and model performance	• Imbalanced data, but solved by sampling techniques such as Random Oversampling	NA	Implementation of new algorithms to replace the repetitive use of sampling and testing

Table 3 (continued)

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[49]	2023	XGBoost	Precision: 97.4%, Recall: 96.8%	European Credit Card Dataset	• Good balance between precision and recall	• Requires extensive hyperparameter tuning	Python	Integration with real-time detection systems
[50]	2023	DT, RF, and LR	Best performance for RF: Accuracy: 0.96, F1-score: 0.17, Recall: 0.97, Precision: 0.09, Specificity: 0.96	Kaggle Western American Credit Card Dataset	• Real-time monitoring • High accuracy	• Computational complexity • Scalability issues	NA	Enhance technique performance
[39]	2024	DT, RF, KNN, and MLP	Achieved 99.97% accuracy	Fraudulent Transaction Datasets	• High accuracy • Handling imbalanced data	• Computational demand for large datasets	Python, Pandas, NumPy, Matplotlib, Seaborn, TensorFlow, Keras, and Scikit-learn	Exploring DL techniques for further improve the detection performance
[40]	2024	Ensemble Learning (SVM, KNN, RF, Boosting)	Highest accuracy of 0.96 for SVM	European Credit Card Transaction Dataset	• Reducing false positives • Robustness to fraud attacks	• Complexity in tuning model parameter	Python	Hybrid models enhancement using supervised and unsupervised methods
[41]	2024	RF, DT, ANN	Highest accuracy achieved for RF equals 98.2%	Public Dataset	• High accuracy and performance	• Computational demand for large data	Python	Exploring ensemble techniques to improve the detection performance
[51]	2024	RF and LR	Accuracy up to 92%	Kaggle Phishing Site URLs Dataset	• High accuracy • Real-time monitoring	• Possible false classifications • Demand for suitable infrastructures to handle big data	Web and Internet	Increase the FD rate
[52]	2024	XGBoost	Precision:97.2%, Recall: 96.8%, Accuracy: 97%, F1-score: 97.4%	Kaggle CCF Dataset	• High, precise Real-time FD • Efficient accuracy	• Computationally intensive • High computational costs	Internet network	Develop hybrid ML models

research articles were chosen that offered methods for identifying a variety of online threats. Essential information and conclusions from these chosen studies have been condensed and are shown in Table 3. This table provides a comprehensive reference for future research and development of FD systems, offering a valuable framework of present research patterns and the reliability of various ML models in the domain.

- DL Models

  In order to address the DL-focused study question, the systematic strategy covered a wide range of recent papers that apply DL methods to enhance CCFD. The scope of this paper includes studies that employ DL's ability to analyze large-scale and complex data, which are features of contemporary digital systems. These academic directions cover a variety of DL architectures, such as CNNs, KNNs, RNNs, and more enhanced models; the substance of these papers, as well as their novel investigations and outcomes, have been succinctly summarized in Table 4. This paper provides researchers with a powerful analytical tool for identifying gaps in the domain of DL technologies in cybersecurity.

- MHO Models

  In regard to the study query on MHO algorithms, we have a collection of published papers that look at the application of these techniques for detecting CCF. The use of MHO algorithms, which are renowned for their capacity to identify ideal or nearly ideal solutions for challenging optimization issues, is growing in the context of improving cybersecurity system detection rates. A variety of MHO techniques, such as bio-inspired optimization and egret swarm optimization, are presented in the research papers selected for review. We have clarified the essence of these papers in Table 5, which summarises their main approaches and conclusions. This table offers a synthesized perspective on the ways in which MHO algorithms are being applied to advance the cutting-edge technology of fraud threat detection, therefore serving as a strategic foundation for further research initiatives in this area.

RQ2: What are the Big Data techniques utilized for CCFD in real time, and what are their limitations and proposed solutions?

Real-time CCFD using big data approaches is essential for correctly and quickly detecting fraudulent transactions. Systems can handle enormous amounts of transactions by utilising ML methods, anomaly detection, and NNs to identify odd trends that can point to fraud. While classification algorithms like DT, LR, and SVM are used to forecast the possibility of fraud based on historical information, strategies like clustering aid in determining the categories of normal vs fraudulent transactions. Ongoing data intake and evaluation are made possible by real-time data processing frameworks like as Apache Spark and Kafka, which guarantee that fraudulent warnings are produced with the least amount of time. Additionaly, advanced DL and ensemble learning methods increase the

Table 4 Recent papers of DL models in CCFD

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[53]	2019	NN, MPL, and CNN	Highest model accuracies: NN: 67.58%, MPL: 87.88%, CNN: 82.86%	Financial Institution Database	• High accuracy • Effective feature sets	• Computationally intensive and resource-consuming • Computational demand for CNN and MPL	NA	Develop complete architecture of a DL model for CCFD
[54]	2019	CNN	Accuracy up to 100% over the training set	Credit Card Transaction Dataset	• Minimized training data • Improved processing time • Decreased recognition rate	• Computational complexity • Overfitting on small training data	NA	Reduction of computational complexity alongside with creating condensed training set
[55]	2020	Combination of DL and ML algorithms: MLP, LR, KNN, NB, RF, and NN	Highest Performance for NN: F1-score: 0.75, Precision: 0.78	ULB Dataset	• Handling complex and high-dimensional data	• Intensive computation • Processing power and large memory requirement	Keras	Enhance the use of the NN algorithm for DL models
[31]	2020	CNN, LSTM, and NLP	Highest F1-score of 84.85% for LSTM	ECD, SCD, and TCD datasets	• Better performance than traditional ML models	• The challenges of newly unseen data • Overfitting and poor generalization	Python (scikit-learn)	Explore hyperparameters to improve the performance of DL models
[56]	2020	NN, LSTM, CNN, Deep & Wide, AdaBM, and LR	AUC scores: 0.8865, 0.8290, 0.8267, 0.8108, 0.8232, and 0.7199	Benchmark Dataset	• Effectiveness in detecting suspicious transactions and fraud patterns	• Computational complexity • Decreased performance for large datasets	NA	Implementing online fraud detection systems instead of offline
[57]	2021	Combination of DL and ML algorithms: ANN, KNN, and SVM	Highest performance for ANN: Accuracy: 0.9993, Recall: 0.7619, Precision: 0.8116	European Bank Dataset from Kaggle	• High accuracy for detecting almost fraud in credit card transactions	• High computational cost • Overfitting	Python, MySQL, and Keras	Enhance the use of NN and DL models across domains
[58]	2021	CNN, AE, LSTM, and AE&LSTM	Accuracies: 0.85, 0.99, 0.85, and 0.32	Credit Card Dataset	• High performance of models, especially AE	• Computationally intensive • Scalability and costs for cloud-based implementation	Google Colab Notebook using Python	Exploring more security methods to detect CCF
[59]	2021	LSTM	Precision: 71%, Recall: 77%, and F1-score: 75%	European and Brazilian Dataset	• High performance of prediction time	• Computational complexity due to LSTM layers • Hardware specifications	Python, and Keras library Hardware: Intel core i7 with 8 GB RAM	Adapting of deep encoder-decoder architectures for CCFD systems

Table 4 (continued)

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[60]	2022	KNN	Highest accuracy of 0.88	Data-driven Dataset	• High efficiency and accuracy	• Adaptability challenge to various data distribution	Python, and MATLAB	Development of DL models predicting novel events
[61]	2024	LSTM, CNN, AutoEncoder	Accuracy: 99.2%, Detection rate: 93.3%	European Credit Card Dataset	• High precision and detection rate	• Hyperparameter tuning complexity • Parameter modification sensitivity	Python (TensorFlow, Keras)	Exploration of more sophisticated hyperparameter tuning
[62]	2024	CNN, LSTM	Accuracy up to 99%	Europe Credit Card Dataset by ULB	• Effectiveness in data protection and security	• Challenges of imbalanced data, real-time detection • Cost of false positives	Python (Scikit-Learn, Pandas, Numpy, Matplotlib, Imblearn, Pytorch, and Syft)	Improve privacy and data protection
[63]	2024	RNN, LSTM, and ANN	Model Accuracy: ANN: 0.9548, LSTM: 0.9571, RNN: 0.9593	European Credit Card Dataset	• High accuracy • Computational efficiency	• Imbalanced data • Handling multiple datasets challenge	Python	Exploration of distributed hyperparameter optimization using the Apache Spark platform
[64]	2024	LSTM, RNN, and CNN	Up to 1.00 accuracy, especially for combined algorithms with LSTM	NAB benchmark Dataset	• High accuracy • High sensitivity • High scalability	• High computational cost • Intensive resources demand	Jupiter Notebook and Python Computer used: Windows 10 Core i7 with 16 GB of RAM	Integration of hybrid models with ML algorithms and real-time processing
[65]	2024	Graph Neural Network (GNN)	Accuracy: 0.97, Precision: 0.82, Recall: 0.92, F1: 0.86,AUROC: 0.92	Sparkov-generated synthetic credit card transactions dataset	• Effective FD • Handling of complex data structure	• Computationally expensive • Implementation complexity at large scale	Sparkov platform	Develop model scaling and handle massive-scale graph
[66]	2024	Deep Neural Network (DNN)	Achieved MCC score of 97.0%	CCF Dataset from Kaggle	• High detection performance of fraudulent transaction detection	• Limited generalization due to dataset specifics	NA	Expand model testing to unbalanced datasets

Table 5 Recent papers of MHO models in CCFD

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[67]	2020	Cuckoo Search Flower Pollination Algorithm (CSFPA)	Accuracy: 96.29% Precision: 0.964 Recall: 0.999	Brazilian Bank Dataset	• Handling misclassification costs	• Computational complexity • Parameter sensitivity	NA	Further evaluation with a large number of datasets
[68]	2020	HPO, RFE, and SMOTE technique	99% as an overall accuracy for the proposed model	Three datasets (European data, PaySim data, and dataset 03)	• High efficiency and accuracy in identifying fraud attacks	• Computationally intensive due to feature selection and data balancing	Python 3.7.1	Study a model on more complex real-world datasets with a high degree of concept drift and imbalanced data
[69]	2021	IEVO, DENN, and HHM	Accuracy up to 0.93	Kaggle Credit Card Dataset	• High accurate rate of FD	• Scalability challenges • Computational complexity	Jupyter Notebook	Enhance optimization to improve model performance
[29]	2022	firefly bio-inspired optimization algorithm and SVM (FFSVM)	Accuracy: 85.65%	Australian Credit Dataset from UCI-ML Repository	• Detection efficiency • Classification accuracy • Handling multimodality	• Computationally intensive due to the bio-inspired technique	Weka Data Mining Framework + Eclipse	Improve classification accuracy by the use of bio-inspired algorithm + DL
[70]	2022	GA integrated with RF, DT, ANN, NB, and LR	Optimal accuracy of 99.98% for GA with RF	European Cardholders Dataset	• High accuracy	• Computationally expensive due to GA	Python, and Scikit-Learn	Utilizing more datasets for the framework validation
[71]	2022	GSFA MHO, Swarm optimization algorithm, SVM, ELM, and XGBoost	The highest accuracy of 99.9842% for the GSFA MHO combined with XGBoost	Kaggle European CCF Dataset	• Decent Performance for highly challenging CCF datasets	• Performance evaluation regarding other NP-hard challenges	Python (Scikit-Learn Library)	Further testing on real-life datasets and NP-hard problems
[72]	2022	Binary Emperor Penguin Optimization (BEPO) with optimal gated recurrent unit (OGRU)	Accuracy of BEPO-OGRU technique is up to 94%	German Credit Card Dataset, and CCFD Dataset	• High classification accuracy	• Computational complexity due to the BEPO algorithm complexity	NA	NA
[73]	2023	ML + Egret Swarm Optimization Algorithm (ESOA)	Accuracy:96.27%, Precision: 16.02% AUC: 73.6%	AAER benchmark dataset by UCB	• High accuracy of financial FD	• Computational complexity and cost due to ESOA's requirements	NA	Enhance hybrid models that combine MHOs with ML
[74]	2024	MHO with ML classifiers	The highest accuracy of 97% for the SFO MHO algorithm	Kaggle European Credit Card Dataset	• High classification accuracy	• Computationally intensive and processing power demand	Python 3.10 and Intel Core i7 with 16 GB RAM	Integrating ML with MHO techniques and DL

Table 5 (continued)

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[75]	2024	Competitive Swarm Optimization (CSO) and Random Weight Network (RWN)	Highest accuracy of 0.993 for the HybridIG-CSO model	Four Datasets from various resources	• Efficiency in FD	• Datasets complexity • Computational power	Python and Intel Core i7 with 8 GB RAM	Use alternative ML techniques for model performance
[76]	2024	BBBO with k-NN, SVM, and Xgb-tree	Highest performance for BBBO with Xgb-tree: ACC: 0.91, and F1: 0.88	10 Benchmark Datasets from UCI repository	• High classification accuracy	• Computational cost • Parameter sensitivity	Python, CPU: intel core i7 with 16 GB of RAM	Integration of BBBO with other MHO for further research

accuracy of fraud detection by identifing the transactions patters, reducing false positives and adapting to new fraud trends.

To overcome the difficulties faced by enormous transaction datasets, the suggested Big Data approach for CCFD integrates real-time stream processing, machine learning methods, and advanced processing tools. According to research studies, Hadoop, Spark, and Kafka frameworks can greatly increase processing speed and accuracy in recognizing fraud (see Table 6). For example, frameworks such as Hadoop and Spark with using ML learning methods give a high accuracy of 90% for a study conducted in 2022 [80] using German Credit Card Dataset. Another example of conducted study in 2017 [82] is achieving low processing time and average speed of 11574 transactions per second which gives 100 million transactions per 24 h.

However, computing restrictions, data imbalance, and reliance on parameter adjustment are some of the drawbacks of using big data methods for CCFD. Although they are limited to single-processor computations, which restricts scalability, methods such as the stochastic stagewise approach provide effective processing of longitudinal data. Two solutions to these issues are the use of hybrid models and distributed processing platforms such as MapReduce and Apache Spark to enable parallel processing. Furthermore, data imbalance is controlled, and the accuracy of the fraudulent detection model is improved by the use of dimensionality reduction techniques like Principal Component Analysis (PCA), data balancing methodologies like balanced RF, and sampling approaches.

Big Data approaches offer high improvement of the detection model performance and accuracy for processing speed, handling massive amount of data, and compatibility with real-time platforms. Incorporating reinforcement learning for adapting detection, investigating semi-supervised learning for utilizing unlabeled samples, and applying DL techniques to enhance further model performance and resiliency against changing fraudulent trends are some suggested future work and proposed solutions to the limitations of Big Data techniques in this area of study.

RQ3: Which datasets are most frequently used to detect CCFD?

The most commonly used datasets for CCFD are summarized as shown in Table 7. The most recent and old datasets for FD are described below, and they show the advantages and some limitations.

Besides the datasets described in the previous table, there are some modern datasets used recently for detecting fraud attacks on credit card transactions that demonstrate distinguish benefits and some limitations, as follows:

1. *CCFD Dataset*: Created in 2023, it contains credit card transactions by European card holders. This dataset contains over 550,000 records, and the data is anonymized to protect the cardholders' information. This dataset aims to improve the algorithms and models to increase the performance of detecting fraudulent transactions. The existing limitation for this dataset is the challenge of class imbalance, as the fraudulent transaction rate is 0.17%, making model training difficult to implement [84]. The extreme class imbalance makes training challenging, potentially resulting in

Table 6 Various studies utilizing Big Data techniques for detecting CCF in real time

Refs.	Year	Methodology	Result	Dataset	Advantages	Limitations	Environment	Future direction
[79]	2020	Stochastic stagewise technique with Big Data	Predictive performance for Model 1: Misc = 0.52% FN = 29.20% FP = 0.16% Model 2: Misc = 0.57% FN = 24.01% FP = 0.27%	Synthetic Credit Card fraud data by BankSim	• Handling longitudinal data in a scalable way • Improved efficiency due to easily integration with other techniques	• Sub-sampling methodology used with stagewise technique is useful for only single processor algorithms	NA	Using the stagewise approach with large datasets over several processors instead of single one
[77]	2021	DL techniques (LSTM with Attention mechanism)	Accuracy of 92% for temporal fraud trends	Public Credit Card Fraud Dataset	• Effective for sequential data • Adaptability to changing fraudulent patterns	• Complicated architecture • Longer training times	Python	Integration of reinforcement learning for adaptive models
[80]	2022	Apache Kafka + ML integration	KNN has the best accuracy of 96.29% for German Data Ridge classifer has the best accuracy of 81.75% for Taiwan Data	German and Taiwan Credit Card Datasets	• High speed processing • Low latency • High accuracy for real-time detection	• Extensive computation due to handling large volumes of data • Imbalanced data challenge	Apache Kafka, Spark	Reinforcement learning exploration for adaptive fraud detection
[70]	2022	ML techniques, GA	Achieved 98% accuracy	European Cardholders' Transactions Dataset	• High accuracy • Effective feature selection	• Significant computation demand for large datasets	Python, Scikit	Exploration of DL methods for improving detection accuracy
[81]	2023	Stream processing in Big Data with supervised and unsupervised filters	Achieved accuracy of 0.987 with PCA dimension reduction	UCI Machine Learning Repository	• High accuracy and scalability in real-time detection	• Dependence on parameter tuning	MapReduce, PCA, LASSO	Enhancement of detection models by integrating DL techniques
[78]	2023	Subspace learning approaches based on class classification	Accuracy of 88% for rare fraud patterns	Kaggle Datasets by ULB	• Handling imbalanced data	• Challenges with various fraudulent types	NA	Exploration of transfer learning for improving generalization across datasets
[40]	2024	Ensemble Learning (SVM, KNN, RF, Boosting)	Highest accuracy of 0.96 for SVM	European Credit Card Transaction Dataset	• Reducing false positives • Robustness to fraud attacks	• Complexity in tuning model parameter	Python	Hybrid models enhancement using supervised and unsupervised methods
[78]	2024	Graph-based techniques (Graph Attention Networks with Dilated Convolutions)	Achieved Accuracies: 2018CN dataset = 0.9712 2023EU dataset = 0.9992	Local Datasets (2018CN, 2023EU)	• Applicability in real-world scenarios • Robust detection performance	• Graph complexity and sparsity	Python 3.12, PyTorch 2.2.0	Exploration of additional graph-based methodologies and expanding its implementation to other financial fraud types

Table 7 Overview of benchmark datasets [83]

Dataset	Year	Records	Benign%	Malicious%
Australian Credit Card Approval	1992	690	55.51%	44.49%
PKDD'99	1999	100 K	95.00%	5.00%
Taiwan Default Credit Card	2005	30 K	77.88%	22.12%
UCSD-FICO	2009	100 K	98.30%	1.70%
Kaggle CCFD	2013	~285 K	99.83%	0.17%
Synthetic Data Generation	2013	500 K	98.00%	2.00%
PaySim	2017	~6 M	97.28%	2.72%
SAS CCF	2017	1 M	99.80%	0.20%
European Central Bank (ECB)	2018	1.5 M	99.50%	0.50%
IEEE-CIS	2019	~1 M	96.90%	3.10%
Vesta Kaggle Dataset	2019	~600 K	97.50%	2.50%
Tsinghua Credit Card	2020	30 K	99.47%	0.53%

higher false negatives, as models may struggle to identify rare fraud cases effectively. Advanced techniques like SMOTE or ensemble methods might be needed to improve recall without sacrificing precision.

2. *IEEE-CIS Fraud Detection Dataset*: Released in 2020, the IEEE-CIS Datasets, in cooperation with Vesta, introduces the best solution for the fraud transaction industry with approximately 590,000 records. It basically works by alerting cardholders in case of fraud attack detection. That can help to save the cardholders' money and increase the revenue yearly. The data comes from Vesta's real-world e-commerce transactions, which have a range of features that improve the efficiency of the alert system, and millions of people will benefit from them. Class imbalance could be a limitation for this dataset, but SMOTE technique or ensemble methods could handle this challenge effectively [85]. This dataset's real-world features, including behavioral attributes, improve model accuracy by enabling better identification of fraud patterns. However, class imbalance remains a limitation, which may necessitate techniques such as cost-sensitive learning to optimize detection without overfitting to majority classes.
3. *FDCompCN Dataset*: This dataset aims to detect financial fraud statements of various companies in China and comes with over 800,000 records. The data are obtained from China Stock Market and Accounting Research, and samples are selected between 2020 and 2023 containing 5,317 listed companies traded on stock exchanges in different Chinese cities. Using the advancement of neural network models, models can learn from data relations, which shows a unique benefit for this dataset. However, the overfitting challenge requires extensive preprocessing and careful feature selections to avoid that problem [86]. The high dimensionality enhances the model's ability to learn complex fraud patterns, but it may also increase the risk of overfitting, especially with neural network-based models. Effective feature selection or dimensionality reduction may be required for reliable results.
4. *eBay E-Commerce Fraud Dataset*: Released in 2022, this dataset thoroughly explains e-commerce fraud incidents with over 1.5 million transactions gathered from eBay's platform. Features like user profiles, transaction histories, and product categories are

significant for building strong FD models, making the dataset useful. However, this dataset's emphasis on e-commerce fraud has an issue as it might not be immediately adaptable for traditional CCFD models. Additionally, processing and analysis of the massive volume of data demand significant computational resources [87]. The dataset's comprehensive e-commerce context and detailed features can enhance model performance for fraud scenarios involving user behavior. However, computational demands may be high due to the data volume, making it suitable for models optimized for big data processing or parallel computing.

5. *Fraudulent Transaction Detection Dataset (FTD)*: Released in 2023, the Fraudulent Transaction Detection (FTD) dataset covers more than 1.75 million transaction records and is intended to identify new fraud patterns in the finance industry. This dataset is very useful for identifying complex and multi-channel fraud schemes since it contains a wide range of variables, including transaction timing, location, merchant information, and client demographics. One noteworthy advantage is that it incorporates the most recent fraud patterns, which are essential for creating models that work in the current fraud environments. However, because of the dataset's imbalance, accurate model training is complex, and the dataset's size and complexity call for thorough preprocessing and feature engineering [88]. The diversity of features allows models to capture current fraud tactics effectively, which is critical for real-time fraud detection. However, the class imbalance and large data size can make preprocessing complex, potentially impacting computational efficiency and model generalization.

Each dataset brings unique strengths and challenges based on its data structure and feature diversity. High-dimensional datasets, such as FDCompCN and FTD, generally enhance the model's fraud detection abilities by providing richer fraud indicators, though they may require preprocessing to avoid overfitting. Real-world transaction data (IEEE-CIS, eBay) often leads to improved fraud pattern detection but requires balancing techniques to manage class imbalance. Each dataset's specific attributes guide model selection and preprocessing choices, which are crucial for optimizing CCFD model performance. A comparative analysis of above-mentioned datasets is illustrated in Table 8, which clarifies how the characteristics of each dataset can affect model performance.

These recent datasets provide significant resources for cybersecurity research, especially in the area of CCFD. That allows for the development and evaluation of enhanced security frameworks and detection models. However, each has distinct challenges that need to be taken into account when applying them to research and applications in the real world.

RQ4: What are the drawbacks of employing ML, DL, and MHO models in CCFD?

- ML Models

  Although ML models have a crucial role in CCF-attacks detection, they come with challenges and limitations that affect their real-world application in the field of cybersecurity, including:

Table 8 Comparative analysis of the used recent datasets for CCFD

Dataset	Year	Records	Key features	Advantages	Limitations	Model performance
CCFD Dataset	2023	550 K	Anonymized European cardholder transactions	Enhancing of fraud detection algorithms	High class imbalance	Accuracy: 70%
IEEE-CIS Fraud Detection Dataset	2020	590 K	Real-word e-commerce transaction data	Fraud Alerts to the cardholders	Class imbalance, but can be handled with techniques	Accuracy: 85%
FDCompCN Dataset	2023	800 K	Financial fraud statement from Chinese companies	Using neural networks for data relation learning	Risk of overfitting and extensive preprocessing	Accuracy: 78%
eBay E-Commerce Fraud Dataset	2022	1.5 M	User profiles, transaction histories, and product categories	Strong feature set and comprehensive e-commerce context	Computationally intensive due to complex feature set and big data	Accuracy: 82%
Fraudulent Transaction Detection Dataset (FTD)	2023	1.75 M	Transaction timing, location, merchant info, and demoographics	Complex fraud patterns capturing and adaptability for current trends	High class imbalance and processing demand	Accuracy: 76%

- *Complexity and interpretability*: Understanding ML models' decision-making process is challenging due to their complicated structure, which is crucial to gaining confidence in cybersecurity [46, 50, 89].
- *Scalability*: Scaling ML models to manage massive data sets and offer real-time analysis is difficult [50].
- *Computational demand*: Significant processing power is required for both training and deploying these models, which represents a problem for systems with low resources [44, 52, 90, 91].
- *Adaptability*: Retraining models to stay up to date with new or evolving attack techniques increases the likelihood that zero-day attacks will go unrecognized [42].
- *Large dataset*: Demands extensive training and precisely labeled data, both of which are frequently difficult to find in the cybersecurity field [47, 48].

These limitations and challenges demonstrate the need for further research into more advanced, adaptable, and sufficient ML methods for detecting fraud attacks.

- DL Models

Despite DL methods and techniques having a high accuracy of fraud-attack detection, there exist some limitations and challenges, as follows:

- *Computational complexity*: This computational complexity comes from complex and advanced DL algorithms used in building the models [54, 56, 64, 65].
- *Resource limitations*: In certain circumstances, it may not be possible to provide sufficient computational resources for practical training and operation [53].

  - *Delayed real-time detection*: High computing demands may slow down real-time detection capabilities [62].
  - *Dataset challenges*: Large training datasets are necessary for DL models, which increases the computational difficulty [63, 66].

- MHO Models
  Although MHO algorithms show unique benefits for their sufficient fraud-attacks detection, they face some limitations, including:

  - *Computational complexity*: They may demand a long time and a lot of computing resources, particularly for large or complex datasets [67, 69, 73].
  - *Scalability issues*: MHO algorithms may have trouble scaling effectively as the dataset gets larger, which could result in a decline in detection accuracy or an increase in calculation time [69].
  - *Parameter sensitivity*: The choice of parameters significantly impacts the performance of MHO algorithms. It can be challenging to enhance these parameters, and it frequently calls for in-depth research or domain experience [61].
  - *Dataset complexity*: Transactions may be misclassified due to the algorithm's inability to efficiently explore the search space and come up with a suitable solution due to the dataset's complexity, which includes high dimensionality, class imbalance, and incomplete data [75].

RQ5: What future directions are recommended for ML, DL, and MHO models in detecting CCF attacks?

- ML Models

  - *Integration with Real-time Fraud Detection*: ML models can be better integrated with real-time FD systems to promptly respond to suspicious transactions without affecting accuracy. Additionally, online learning strategies that can adjust to new data as it comes in can be studied to help the model identify emerging fraud patterns [46, 49].
  - *Improvement of Detection Systems*: Modern technologies will be included in a new ML-based detection system to enhance attack identification, handle anomalies, and manage high-dimensional data, resulting in a reliable and effective cybersecurity solution [42, 45].
  - *Handling Imbalanced Data*: The class imbalance in CCFD datasets can be solved by implementing sophisticated resampling strategies or cost-sensitive learning methods. Additionally, new algorithms that are less susceptible to data imbalance may be investigated to lower the risk of model bias [44, 91, 92].
  - *Hybrid Models Approach*: Investigating hybrid models that combine conventional ML algorithms with alternative strategies, like DL or MHOs, capitalizing on the advantages of each approach, as well as creating ensemble methods that incorpo-

rate several models to increase detection robustness and accuracy, especially in complex fraud scenarios [46, 52].

- DL Models
  - *Development of Architecture*: To improve detection accuracy, develop hybrid models that integrate DL with other techniques, such as statistical methods or classical ML. New DL structures, such as transformers and graph neural networks, are being studied to capture more complicated interactions in transaction data [53, 59].
  - *Handling Large-scale Data*: The large volumes of data produced by financial transactions can be processed and analyzed more effectively by optimizing DL models. Additionally, federated learning approaches can train DL models on distributed data sources without affecting privacy [54].
  - *Hybrid Models*: Further work might merge AI and DL to build models that integrate learning and reasoning, leveraging neural-symbolic systems to improve interpretability and adaptability [64].
  - *Neural Network Algorithm*: Studying novel or enhanced neural network algorithms designed especially for FD applications, with an emphasis on improving the algorithms' capacity to learn from intricate, high-dimensional data. Furthermore, it has been shown that improving neural network architectures—like deep convolutional or recurrent networks—improves their ability to identify fraudulent patterns [55, 57].
  - *Hyperparameter Optimization*: Using automated hyperparameter tuning techniques, like grid search, random search, or Bayesian optimization, to find the optimal model configurations and concentrating on hyperparameter optimization techniques to fine-tune DL models, thereby increasing their accuracy and generalization on FD tasks [31, 61, 63].

- MHO Models
  - *Integration of MHO Algorithms*: Utilizing several MHO algorithms together (such as ant colony optimization, simulated annealing, and GAs) to improve feature selection techniques [74, 76].
  - *Hybrid Models Approach*: Investigating hybrid approaches that mix filter-based and wrapper-based methods with MHO algorithms to benefit from the advantages of several approaches for increased efficiency and accuracy [73].
  - *Addressing Dataset Complexity*: Developing adaptive algorithms that can successfully navigate complicated search spaces and avoid becoming stuck in local optima, as well as developing MHO algorithms that can better manage the challenges of CCFD datasets, such as high dimensionality, noise, and class imbalance [68].
  - *Classification Accuracy*: Integrating MHOs to optimize the classification model to maximize the model's accuracy in identifying fraudulent and authentic transactions [29].

Conclusion

The study has successfully analyzed various AI-driven CCFD methods in this in-depth investigation. Our assessment was derived from the first set of 628 papers, which got a thorough analysis based on keywords, titles, and abstracts. A rigorous selection of inclusion and exclusion criteria produced 52 research papers that matched our high standards. To ensure a focused source of studies for additional analysis, crucial details, including publication specifics, citation measures, research areas, techniques, and datasets, were mainly taken from each work's preliminary parts. Most of these studies concentrate on sophisticated methods like DL, ML, and MHO methodologies. We offer a thorough comparison of ML, DL, and MHO models by analyzing them, exposing the advantages and drawbacks of current CCFD frameworks. Our investigation reveals major problems that existing AI models must deal with, especially those related to data imbalance and high processing demands. ML models like Random Forest (RF) and Support Vector Machine (SVM) demonstrate strong classification capabilities but are challenged by issues like data imbalance and scalability in real-time applications. Ensemble methods and hybrid models that combine ML with other techniques show promise for improving accuracy. DL models, especially CNNs and LSTMs, excel in capturing complex patterns, making them suitable for high-dimensional data. However, they often demand substantial computational resources and are prone to overfitting with limited data, highlighting the need for efficient training techniques and model regularization. MHO algorithms, such as Genetic Algorithms and Particle Swarm Optimization, improve feature selection and model tuning, enhancing detection rates. While effective, these methods can be computationally intensive and require careful parameter tuning, making them challenging for large datasets or real-time scenarios. Notably, despite ongoing problems with scalability and parameter tuning, the optimisation of MHO algorithms presents a viable path towards improving the detection rate.

In the future, we tend to analyze and investigate these topics:

- *Hybrid and Ensemble Models:* Combining ML, DL, and MHO techniques in hybrid architectures can leverage the strengths of each method, improving detection accuracy, reducing false positives, and enabling real-time analysis. These hybrid models that combine the best features of several AI techniques could greatly advance CCFD in the future by maximizing detecting fraud performance while resolving class imbalance and real-time processing needs. Such hybrid approaches could integrate Big Data technologies to address the scalability challenges in processing large transaction volumes.
- *Handling Class Imbalance*: Research should continue exploring advanced resampling methods and algorithms less sensitive to class imbalance. Investigating semi-supervised or active learning methods may also help use unlabeled data effectively, improving model robustness without over-reliance on labeled instances.
- *Optimization and Real-Time Adaptability*: Developing adaptive models that self-update based on new fraud patterns is crucial for CCFD's evolving landscape. Integrating reinforcement learning or meta-learning with MHO algorithms could offer dynamic solutions capable of adjusting to emerging threats.

- *Interpretable AI and Model Transparency*: As CCFD models become more complex, improving model interpretability and transparency is essential. Enhanced explainability will aid both analysts and end-users in understanding and trusting AI-driven fraud detection systems.
- *Creation of powerful and flexible models in CCFD*: Through the utilization of more recent, reliable datasets, opening the door for efficient defences against changing fraud strategies. This work lays a solid basis for further investigation, highlighting the significance of ongoing developments in AI techniques to guarantee safe financial transactions in a world that is increasingly becoming more digital.

Abbreviations

AI	Artificial Intelligence
ANN	Artificial Neural Network
APT	Advanced persistent threat
BBBO	Binary brown-bear optimization
CCF	Credit card fraud
CCFD	Credit card fraud detection
CNN	Convolutional Neural Network
CSFPA	Cuckoo Search Flower Pollination Algorithm
CSO	Competitive swarm optimization
DENN	Differential Evolution-based Neural Network
DL	Deep learning
DM	Data Mining
DT	Decision Tree
ELM	Extreme Learning Machine
ESOA	Egret Swarm Optimization Algorithm
FD	Fraud Detection
FFSVM	Firefly and Feature optimization with SVM
FL	Fuzzy Logic
GA	Genetic Algorithm
GB	Gradient Boosting
GNN	Graph Neural Network
GSFA	Guided Search Fireworks Algorithm
HHM	Hybrid Heuristic and Meta-Heuristic Algorithm
HM	Hybrid methods
HPO	Hyper-parameter optimization
IEVO	Improved Egyptian Vulture Optimization
KNN	K-Nearest Neighbors
LC	Linear Classifiers
LOF	Local Outlier Factor
LR	Logistic Regression
LSTM	Long Short-Term Memory
MBO	Migrating Birds Optimization
MHO	Meta-heuristic Optimization
ML	Machine Learning
MLP	Multilayer Perceptron
MPL	Meta Pseudo Labels
NB	Naïve Bayes
NLP	Natural Langauge Processing
RF	Random Forest
RFE	Recursive Feature Elimination
RNN	Recurrent Neural Network
RWN	Random Weight Network
SVM	Support Vector Machines

Acknowledgements
Not applicable.

Author contributions
Conceptualization, literature review, discussion, writing—original draft preparation: IY.H, AY.H, and AM.A; data downloading: IY.H, AY.H, ABE, and AAA; writing—review and editing: AM.A, ABE, and AAA; visualization: Y.H, AY.H, and ABE; supervision: ABE, and AAA. All authors read and approved the final manuscript.

Funding
Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). No funds are available for this research.

Data availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Received: 21 September 2024 Accepted: 14 December 2024
Published online: 14 January 2025

References

1. Parkar P, Bilimoria A. A survey on cyber security IDS using ML methods. 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 352–360, 2021. https://api.semanticscholar.org/CorpusID:235208042.
2. Musa N, Mirza N, Rafique S, Abdallah A, Murugan T. machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions. IEEE Access. 2024. https://doi.org/10.1109/ACCESS.2024.3360868.
3. Eswaran M, Hamsanandhini S, Lakshmi KI. Survey of cyber security approaches for attack detection and prevention. Turk J Comput Math Educ. 2021;12(2):3436–41. https://www.proquest.com/scholarly-journals/survey-cyber-security-approaches-attack-detection/docview/2624698524/se-2.
4. Barik K, Misra S, Konar K, Fernandez-Sanz L, Koyuncu M. Cybersecurity deep: approaches, attacks dataset, and comparative study. Appl Artif Intell. 2022. https://doi.org/10.1080/08839514.2022.2055399.
5. Morovat K, Panda B. A survey of artificial intelligence in cybersecurity. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 109–115. https://doi.org/10.1109/CSCI51800.2020.00026.
6. Rauf U, Mohsen F, Wei Z. A taxonomic classification of insider threats: existing techniques, future directions & recommendations. J Cyber Secur Mobil. 2023;12(2):221–52. https://doi.org/10.13052/jcsm2245-1439.1225.
7. Thanh Vu SN, Stege M, El-Habr PI, Bang J, Dragoni N. A survey on botnets: incentives, evolution, detection and current trends. Future Internet. 2021. https://doi.org/10.3390/fi13080198.
8. Abu Bakar A, Zolkipli MF. Cyber security threats and predictions: a survey. Int J Adv Eng Manag IJAEM. 2023;5:73. https://doi.org/10.35629/5252-0502733741.
9. Parizad A, Hatziadoniu CJ. Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework. IEEE Trans Smart Grid. 2022. https://doi.org/10.1109/TSG.2022.3176311.
10. Richmond HT. Philosophical logic and artificial intelligence. Springer Netherlands, 1989. https://doi.org/10.1007/978-94-009-2448-2.
11. Pomerol J-C. Artificial intelligence and human decision making. Eur J Oper Res. 1997;99(1):3–25. https://doi.org/10.1016/S0377-2217(96)00378-5.
12. Li J. Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng. 2018;19(12):1462–74. https://doi.org/10.1631/FITEE.1800573.
13. Welukar JN, Bajoria GP. Artificial Intelligence in cyber security—a review. Int J Sci Res Sci Technol. 2021. https://doi.org/10.32628/IJSRST218675.
14. Thomas T, Vijayaraghavan AP, Emmanuel S. Machine learning approaches in cyber security analytics. Springer Singapore. 2019. https://doi.org/10.1007/978-981-15-1706-8.
15. Kuntla GS, Tian X, Li Z. Security and privacy in machine learning: a survey. Issues Inf Syst. 2021;22(3):224–40. https://doi.org/10.48009/3_iis_2021_242-258.
16. Osisanwo FY, Akinsola JET, Awodele O, Hinmikaiye JO, Olakanmi O, Akinjobi J. Supervised machine learning algorithms: classification and comparison. Int J Comput Trends Technol. 2017;48(3):128–38. https://doi.org/10.14445/22312803/IJCTT-V48P126.
17. Sarker IH, Kayes ASM, Badsha S, Alqahtani H, Watters P, Ng A. Cybersecurity data science: an overview from machine learning perspective. J Big Data. 2020;7(1):41. https://doi.org/10.1186/s40537-020-00318-5.
18. Rodriguez E, Otero B, Gutiérrez N, Canal R. A survey of deep learning techniques for cybersecurity in mobile networks. IEEE Commun Surv Tutor. 2021. https://doi.org/10.1109/COMST.2021.3086296.
19. Pourafshin F. Big Data Mining in Internet of Things Using Fusion of Deep Features. Int J Sci Res Eng Trends. 2021;7(2):1089–93. https://www.researchgate.net/publication/350942227_Big_Data_Mining_in_Internet_of_Things_Using_Fusion_of_Deep_Features.

20. Gu H, Wang Y, Hong S, Gui G. Blind channel identification aided generalized automatic modulation recognition based on deep learning. IEEE Access. 2019;7:110722–9. https://doi.org/10.1109/ACCESS.2019.2934354.
21. Glatstein I, Chavez-Badiola A, Curchoe C. New frontiers in embryo selection. J Assist Reprod Genet. 2023. https://doi.org/10.1007/s10815-022-02708-5.
22. Hassan IH, Mohammed A, Masama MA. Chapter 6—Metaheuristic algorithms in network intrusion detection. In: Mirjalili S, Gandomi AH, editors. Comprehensive metaheuristics. Academic Press; 2023. p. 95–129. https://doi.org/10.1016/B978-0-323-91781-0.00006-5.
23. Rajwar K, Deep K, Das S. An exhaustive review of the metaheuristic algorithms for search and optimization: taxonomy, applications, and open challenges. Artif Intell Rev. 2023;56(11):13187–257. https://doi.org/10.1007/s10462-023-10470-y.
24. Agrawal P, Abutarboush HF, Ganesh T, Mohamed AW. Metaheuristic algorithms on feature selection: a survey of one decade of research (2009–2019). IEEE Access. 2021;9:26766–91. https://doi.org/10.1109/ACCESS.2021.3056407.
25. Saddam Hussain SK, Sai Charan Reddy E, Akshay KG, Akanksha T. Fraud detection in credit card transactions using SVM and random forest algorithms. In 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1013–1017. https://doi.org/10.1109/I-SMAC52330.2021.9640631.
26. BinSulaiman R, Schetinin V, Sant P. Review of machine learning approach on credit card fraud detection. Hum-Centric Intell Syst. 2022. https://doi.org/10.1007/s44230-022-00004-0.
27. Aziz A, Ghous H. Fraudulent transactions detection in credit card by using data mining methods: a review. Int J Sci Prog Res. 2021;179:1.
28. Ali A, et al. Financial fraud detection based on machine learning: a systematic literature review. Appl Sci. 2022. https://doi.org/10.3390/app12199637.
29. Singh A, Jain A, Biable S. Financial fraud detection approach based on firefly optimization algorithm and support vector machine. Appl Comput Intell Soft Comput. 2022;2022:1–10. https://doi.org/10.1155/2022/1468015.
30. Behera T, Panigrahi S. Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network. 2015, pp. 494–499. https://doi.org/10.1109/ICACCE.2015.33.
31. Nguyen TT, Tahir H, Abdelrazek M, Babar A. Deep learning methods for credit card fraud detection. CoRR, vol. abs/2012.03754, 2020. https://arxiv.org/abs/2012.03754.
32. Misra S, Thakur S, Ghosh M, Saha S. An autoencoder based model for detecting fraudulent credit card transaction. Procedia Comput Sci. 2020;167:254–62. https://doi.org/10.1016/j.procs.2020.03.219.
33. Schlör D, Ring M, Krause A, Hotho A. Financial fraud detection with improved neural arithmetic logic units. 2021, pp. 40–54. https://doi.org/10.1007/978-3-030-66981-2_4.
34. Buschjager S, Honysz P-J, Morik K. Randomized outlier detection with trees. Int J Data Sci Anal. 2022;13:1–14. https://doi.org/10.1007/s41060-020-00238-w.
35. Benchaji I, Douzi S, El Ouahidi B. Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection. In: Khoukhi F, Bahaj M, Ezziyyani M, editors. Smart data and computational intelligence: proceedings of the international conference on advanced information technology, services and systems. Cham: Springer International Publishing; 2019. p. 220–9. https://doi.org/10.1007/978-3-030-11914-0_24.
36. Özçelik M, Isik M, Duman E, Cevik T. Improving a credit card fraud detection system using genetic algorithm. ICNIT 2010—2010 International Conference on Networking and Information Technology, 2010. https://doi.org/10.1109/ICNIT.2010.5508478.
37. Kitchenham B, Charters S. Guidelines for performing systematic literature reviews in software engineering. 2, 2007.
38. Gupta P, Varshney A, Khan MR, Ahmed R, Shuaib M, Alam S. Unbalanced credit card fraud detection data: a machine learning-oriented comparative study of balancing techniques. Procedia Comput Sci. 2023;218:2575–84. https://doi.org/10.1016/j.procs.2023.01.231.
39. Talukder MdA, Hossen R, Uddin MA, Uddin MN, Acharjee UK. Securing transactions: a hybrid dependable ensemble machine learning model using IHT-LR and grid search. Cybersecurity. 2024. https://doi.org/10.1186/s42400-024-00221-z.
40. Khalid AR, Owoh N, Uthmani O, Ashawa M, Osamor J, Adejoh J. Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data Cogn Comput. 2024. https://doi.org/10.3390/bdcc8010006.
41. Sonwane VR, Zanje S, Yenpure S, Gunjal Y, Kulkarni Y, Yeole R. Advanced machine learning techniques for credit card fraud detection: a comprehensive study. In 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), 2024, pp. 1978–1981. https://doi.org/10.1109/ICOSEC61587.2024.10722667.
42. Varmedja D, Karanovic M, Sladojevic S, Arsenovic M, Anderla A. Credit card fraud detection—machine learning methods. 2019, pp. 1–5. https://doi.org/10.1109/INFOTEH.2019.8717766.
43. Dornadula VN, Geetha S. Credit card fraud detection using machine learning algorithms. Procedia Comput Sci. 2019;165:631–41. https://doi.org/10.1016/j.procs.2020.01.057.
44. Thennakoon A, Chee B, Premadasa S, Mihiranga S, Kuruwitaarachchi N. Real-time credit card fraud detection using machine learning. 2019. https://doi.org/10.1109/CONFLUENCE.2019.8776942.
45. Itoo F, Mittal M, Singh S. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. Int J Inf Technol. 2020. https://doi.org/10.1007/s41870-020-00430-y.
46. Bagga S, Goyal A, Gupta N, Goyal A. Credit card fraud detection using pipeling and ensemble learning. Procedia Comput Sci. 2020;173:104–12. https://doi.org/10.1016/j.procs.2020.06.014.
47. Alemad M. Credit card fraud detection using machine learning. 2022. https://repository.rit.edu/theses.
48. Valavan M, Rita S. Predictive-analysis-based machine learning model for fraud detection with boosting classifiers. Comput Syst Sci Eng. 2023;45(1):231–45. https://doi.org/10.32604/csse.2023.026508.
49. Goyal R, Manjhvar A, Sejwar V. Credit card fraud detection in data mining using XGBoost classifier. Int J Recent Technol Eng (IJRTE). 2020;9:603–8. https://doi.org/10.35940/ijrte.F8182.059120.
50. Afriyie J, et al. A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decis Anal J. 2023;6: 100163. https://doi.org/10.1016/j.dajour.2023.100163.
51. Singh A, ShibargattiMahasmrti A, Jena A, Manvi S. Machine learning based detection of phishing websites in chrome. AIP Conf Proc. 2024;2742(1): 020072. https://doi.org/10.1063/5.0184539.

52. Kumar BS, Yadav PP, Reddy MR. An intelligent approach to detect and predict online fraud transaction using XGBoost algorithm. Indones J Electr Eng Comput Sci. 2024;35(3):1491–8. https://doi.org/10.11591/ijeecs.v35.i3.pp1491-1498.
53. Sadgali I, Sael N, Benabbou F. Fraud detection in credit card transaction using neural networks. In ACM International Conference Proceeding Series, Association for Computing Machinery, Oct. 2019. https://doi.org/10.1145/3368756.3369082.
54. Ragha Vardhani P, Indira Priyadarshini Y, Narasimhulu Y. CNN data mining algorithm for detecting credit card fraud. In: Muppalaneni NB, Ma M, Gurumoorthy S, editors. Soft computing and medical bioinformatics. Singapore: Springer Singapore; 2019. p. 85–93. https://doi.org/10.1007/978-981-13-0059-2_10.
55. Azhan M, Meraj S. Credit card fraud detection using machine learning and deep learning techniques. In Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020, Institute of Electrical and Electronics Engineers Inc. 2020, pp. 514–518. https://doi.org/10.1109/ICISS49785.2020.9316002.
56. Cheng D, Xiang S, Shang C, Zhang Y, Yang F, Zhang L. Spatio-temporal attention-based neural network for credit card fraud detection. www.aaai.org.
57. Rb A, Kr SK. Credit card fraud detection using artificial neural network. Glob Trans Proc. 2021;2(1):35–41. https://doi.org/10.1016/j.gltp.2021.01.006.
58. Hussein D, Ibrahim D, Alshobaili J, Aloufi A, Almuteer A, Alrashidi W. Detecting credit card fraud using machine learning. Int J Interact Mobile Technol (iJIM). 2021;15:108–22. https://doi.org/10.3991/ijim.v15i24.27355.
59. Forough J, Momtazi S. Ensemble of deep sequential models for credit card fraud detection. Appl Soft Comput. 2021;99:106883. https://doi.org/10.1016/j.asoc.2020.106883.
60. Alammar A, Al Moaiad Y, Algeelani N. Transaction fraud detector using KNN in deep learning. 2022;9:16–23. https://doi.org/10.5281/zenodo.7365019.
61. Sumaya SMH, Sulaiman Ibraheem Nadher S. Credit card fraud detection using improved deep learning models. Comput Mater Continua. 2024;78(1):1049–69. https://doi.org/10.32604/cmc.2023.046051.
62. Baabdullah T, Alzahrani A, Rawat DB, Liu C. Efficiency of federated learning and blockchain in preserving privacy and enhancing the performance of Credit Card Fraud Detection (CCFD) Systems. Future Internet. 2024. https://doi.org/10.3390/fi16060196.
63. El Kafhali S, Tayebi M, Sulimani H. An optimized deep learning approach for detecting fraudulent transactions. Information. 2024. https://doi.org/10.3390/info15040227.
64. Iqbal A, Amin R. Time series forecasting and anomaly detection using deep learning. Comput Chem Eng. 2023;182:108560. https://doi.org/10.1016/j.compchemeng.2023.108560.
65. Cherif A, Ammar H, Kalkatawi M, Alshehri S, Imine A. Encoder–decoder graph neural network for credit card fraud detection. J King Saud Univ Comput Inf Sci. 2024. https://doi.org/10.1016/j.jksuci.2024.102003.
66. Shome N, Sarkar DD, Kashyap R, Lasker RH. Detection of credit card fraud with optimized deep neural network in balanced data condition. Comput Sci. 2024. https://doi.org/10.7494/csci.2024.25.2.5967.
67. Singh A, Jain A. Cost-sensitive metaheuristic technique for credit card fraud detection. J Inf Optim Sci. 2020;41(6):1319–31. https://doi.org/10.1080/02522667.2020.1809090.
68. Rtayli N, Enneya N. Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. J Inf Secur Appl. 2020;55: 102596. https://doi.org/10.1016/j.jisa.2020.102596.
69. Shahapurkar A. Accurate fraud detection in credit card transactions using hybrid heuristic and meta-heuristic algorithms. SSRN Electron J. 2021. https://doi.org/10.2139/ssrn.3834947.
70. Ileberi E, Sun Y, Wang Z. A machine learning based credit card fraud detection using the GA algorithm for feature selection. J Big Data. 2022. https://doi.org/10.1186/s40537-022-00573-8.
71. Jovanovic D, Antonijevic M, Stankovic M, Zivkovic M, Tanaskovic M, Bacanin N. Tuning machine learning models using a group search firefly algorithm for credit card fraud detection. Mathematics. 2022. https://doi.org/10.3390/math10132272.
72. Arun GK, Rajesh P. Design of metaheuristic feature selection with deep learning based credit card fraud detection model. In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2022, pp. 191–197. https://doi.org/10.1109/ICAIS53314.2022.9742937.
73. Yi Z, et al. Fraud detection in capital markets: a novel machine learning approach. Expert Syst Appl. 2023;231: 120760. https://doi.org/10.1016/j.eswa.2023.120760.
74. Mosa DT, Sorour SE, Abohany AA, Maghraby FA. CCFD: efficient credit card fraud detection using meta-heuristic techniques and machine learning algorithms. Mathematics. 2024;12(14):2250. https://doi.org/10.3390/math12142250.
75. Faisal E, Ahmad H, Zaghloul R. Efficient credit card fraud detection using evolutionary hybrid feature selection and random weight networks. Int J Data Netw Sci. 2024. https://doi.org/10.5267/j.ijdns.2023.9.009.
76. Sorour SE, AlBarrak KM, Abohany AA, El-Mageed AAA. Credit card fraud detection using the brown bear optimization algorithm. Alex Eng J. 2024;104:171–92. https://doi.org/10.1016/j.aej.2024.06.040.
77. Benchaji I, Douzi S, El Ouahidi B, Jaafari J. Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. J Big Data. 2021. https://doi.org/10.1186/s40537-021-00541-8.
78. Zaffar Z, Sohrab F, Kanniainen J, Gabbouj M. Credit card fraud detection with subspace learning-based one-class classification. 2023. http://arxiv.org/abs/2309.14880
79. Vaughan G. Efficient big data model selection with applications to fraud detection. Int J Forecast. 2020;36(3):1116–27. https://doi.org/10.1016/j.ijforecast.2018.03.002.
80. Saheed YK, Baba UA, Raji MA. Big data analytics for credit card fraud detection using supervised machine learning models. In: Sood K, Balusamy B, Grima S, Marano P, editors. Big data analytics in the insurance market. Bingley: Emerald Publishing Limited; 2022. p. 31–56. https://doi.org/10.1108/978-1-80262-637-720221003.
81. Banirostam H, Banirostam T, Pedram MM, Rahmani AM. A model to detect the fraud of electronic payment card transactions based on stream processing in Big Data. J Signal Process Syst. 2023;95(12):1469–84. https://doi.org/10.1007/s11265-023-01903-6.
82. Dai Y, Yan J, Tang X, Zhao H, Guo M. Online credit card fraud detection: a hybrid framework with big data technologies. In 2016 IEEE Trustcom/BigDataSE/ISPA, 2016, pp. 1644–1651. https://doi.org/10.1109/TrustCom.2016.0253.

83. Priscilla DP, Victoria C, Prabha. Credit card fraud detection: a systematic review. In Jain LC, S-L Peng, Alhadidi, Souvika S, editors. Intelligent Computing Paradigm and Cutting-edge Technologies, Cham: Springer International Publishing; 2020, pp. 290–303.
84. Elgiriyewithana N. Credit card fraud detection dataset 2023. Kaggle. https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023. Accessed 5 Sep 2024.
85. Howard A, Bouchon-Meunier B, Lei J, Abbass H. IEEE-CIS fraud detection. Kaggle. https://kaggle.com/competitions/ieee-fraud-detection. Accessed 5 Sep 2024.
86. Wu B, Yao X, Zhang B, Chao K-M, Li Y. SplitGNN: spectral graph neural network for fraud detection against heterophily. 2023, pp. 2737–2746. https://doi.org/10.1145/3583780.3615067.
87. Rao SX, Zhang S, Han Z, Zhang Z, Min W, Chen Z, Shan Y, Zhao Y, Zhang C. xFraud: explainable fraud transaction detection. Proc VLDB Endowm. 2021;15(3):427–36. https://doi.org/10.14778/3494124.3494128.
88. Singh S. Fraudulent transaction detection. Kaggle. [https://www.kaggle.com/datasets/sanskar457/fraud-transaction-detection. Accessed 5 Sep 2024.
89. Jain R, Gour B, Dubey S. A hybrid approach for credit card fraud detection using rough set and decision tree technique. 2016.
90. Noghani FF, Moattar M-H. Ensemble classification and extended feature selection for credit card fraud detection. 2017.
91. Awoyemi J, Adetunmbi A, Oluwadare S. Credit card fraud detection using machine learning techniques: a comparative analysis. 2017. pp. 1–9. https://doi.org/10.1109/ICCNI.2017.8123782.
92. Xuan S, Liu G, Li Z, Zheng L, Wang S, Jiang C. Random forest for credit card fraud detection. Institute of Electrical and Electronics Engineers. 2018; p. 127. https://doi.org/10.1109/ICNSC.2018.8361343.

Publisher's Note