Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

A Systematic Review Of Credit Card Fraud Detection And Prevention Techniques

Marouane Ben Boubker[1], Ahmed Eddaoui[2], Sara Ouahabi[3], Kamal El Guemmat[4], Tarik Chafik[5]

[1]Faculty of Science Ben M'Sik,University Hassan II, Casablanca, Morocco
[2]Faculty of Economic and Social Juridical Sciences Ain Sebaâ, Casablanca, Morocco
[3]Faculty of Science Ben M'Sik, University Hassan II, Casablanca, Morocco
[4]Faculty of Science Ben M'Sik, University Hassan II, Casablanca, Morocco
[5]Faculty of Science Ben M'Sik, University Hassan II, Casablanca, Morocco
Corresponding Author:
Marouane BEN BOUBKER
Information processing laboratory, Faculty of Science Ben M'Sik,University Hassan II
Casablanca, Morocco
Email: marouane.benboubker@gmail.com

The data science community has shown significant interest in credit card fraud (CCF) due to its growing prevalence and the significant financial losses it causes. However, existing systematic reviews have not thoroughly explored the various techniques used in CCF beyond mere comparisons.

The objective of this research is threefold. First and foremost, it aims to provide a clear definition and classification of CCF. Furthermore, it aims to provide a comprehensive overview of the standard techniques currently employed to prevent CCF, ensuring strict adherence to industry and international payment network standards. The study also seeks to explore alternative tools proposed in existing literature. Lastly, the research aims to conduct a systematic analysis of advanced techniques using different aspects of machine learning and deep learning models. This analysis includes considering the type of model, estimation metrics, model comparison, as well as the challenges encountered during the process.

A comprehensive search was conducted across multiple electronic databases to review studies published between 1990 and 2021. The review concentrated on two primary categories: studies focused on the classification of credit card fraud and those that examined the key techniques used for its prevention and detection.

Deep learning (DL) models show great potential in the detection and prevention of CCF. However, their use in industry remains limited, highlighting the need for further efforts and incentives to support their implementation. Based on our review, we offer targeted recommendations for researchers and practical guidelines for industry professionals.

Keywords: Financial Fraud Credit Card Fraud Security Protocol Data Mining Machine Learning Deep Learning

1. INTRODUCTION

Credit card fraud is a widespread and serious problem that financial institutions are working hard to combat. Beyond the significant financial losses, this type of fraud damages the credibility of both the institutions and the broader financial ecosystem.

Classic tools and conventional approaches have been extensively implemented to combat credit card fraud. However, their effectiveness has been constrained, as fraudsters have leveraged new technologies to discover novel avenues for fraud while maintaining anonymity. This is particularly evident in electronic payment systems where the physical presence of the card is not required.

Financial institutions have recognized the importance of incorporating Machine Learning techniques to enhance the security of their systems, leading to favorable outcomes. However, these techniques have exhibited limitations, particularly when confronted with complex and extensive datasets or when applied in real-time scenarios. Deep Learning, on the other hand, offers more advanced methodologies to address these limitations and deliver enhanced accuracy and performance. Nevertheless, the selection between Machine Learning and Deep Learning techniques is not straightforward and necessitates a comprehensive justification that encompasses all the challenging aspects of credit card fraud.

The motivation behind this survey is to conduct a thorough examination of the problem of CCF and its challenging aspects. The objective is to propose a comprehensive analysis of the current trends in CCF detection techniques, offering a cross-sectional perspective and conducting a comparative study using different criteria and methods. The distinct motivation for undertaking this comprehensive review can be summarized as follows:

- To understand CCF phenomenon and its taxonomy
- To study the standard tools and conventional approaches used for CCF detection and prevention
- To study security protocols for electronic payment transaction
- To conduct a study on Machine Learning and Deep Learning techniques applied to CCF prevention and detection
- To study the challenging areas while applying learning algorithms

Our contribution consists of

- To develop a profound understanding of the CCF phenomenon
- To delve into the challenges posed by CCF
- To provide a state of the art of the security protocols implemented in the industry as well as the suggested ones in the litterature
- A comparative analysis of all the methods based on different evaluation metrics to assess and compare the performance of various methods in addressing CCF problems.

1.1. Article organization

The article is structured as follows: Section 1 introduces the topic and outlines the motivation and objectives of the study. Section 2 details the review methodology, including the selection of sources and search criteria. Section 3 addresses the challenge of imbalanced data in credit card fraud detection, reviewing relevant literature. Section 4 explores various approaches to managing imbalanced data, while Section 5 provides a comparative analysis of machine learning algorithms used in fraud detection.

Section 6 discusses performance metrics for evaluating models, and Section 7 reviews the key findings and limitations of existing solutions. Section 8 highlights open issues and challenges in the field, leading to Section 9, which concludes with a summary of insights and recommendations for future research and practice. This structure ensures a logical flow from introduction to conclusion, covering both theoretical and practical aspects of credit card fraud detection.

2. FINANCIAL FRAUD

2.1. Taxonomy of Financial Fraud

Financial fraud encompasses deceptive actions taken by a perpetrator with the intention of obtaining unauthorized gains or depriving a victim of their rights [1]. This can involve various deceptive tactics employed to access illegal gains or deny the victim their rightful entitlement. According to Arushi Jain (2019) [2], financial fraud can be classified into four primary categories:

- **Bank fraud** involves the use of illegal tactics by fraudsters to unlawfully acquire funds or assets.
- **Insurance fraud** involves any deliberate action taken to deceive an insurance process. This can happen when individuals seek benefits they aren't eligible for or when an insurer wrongfully withholds legitimate entitlements.
- **Securities and commodities fraud**, often called speculation or stock market fraud, refers to dishonest practices involving investments and trading within securities and commodities markets.
- **Other types of financial fraud** include all forms not covered in the previous categories, such as corporate fraud and mass marketing scams.

The central area of our focus is CCF, which is classified under bank fraud. This type of fraud holds significant prominence as it is considered the most dominant form within the realm of bank fraud. Moreover, CCF is rapidly escalating and evolving, making it an increasingly critical issue that requires attention and proactive measures.

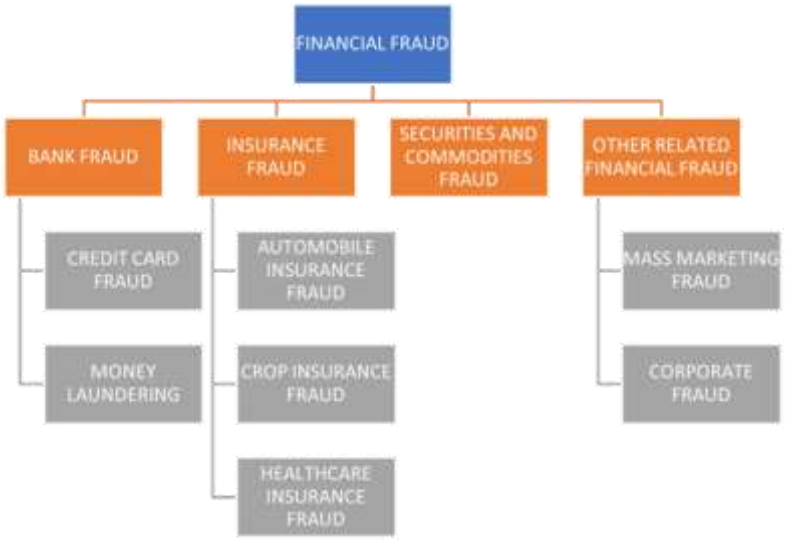

Figure 1 Financial Fraud Taxonomy [1]

2.2. CCF Definition

CCF involves engaging in fraudulent activities using a payment card, such as a credit card, debit card, or prepaid card. The intention behind such fraud can vary, ranging from acquiring goods or services to making payments into an account that is under the control of a criminal. CCF can be categorized into two main types: application fraud and behavioral fraud [3].

Application fraud is a type of financial deception where individuals or fraudsters obtain new payment cards from issuers by submitting false personal information. The goal behind this fraud is to acquire cards with no intention of repaying the charges made on them.

Behavioral fraud includes various fraudulent activities such as counterfeit card fraud, stolen or lost card fraud, mail intercept fraud, and Card Not Present (CNP) fraud, commonly seen in mail or telephone orders.

- Counterfeit card fraud involves creating and using fake cards to conduct unauthorized transactions.
- Stolen or lost card fraud occurs when a genuine card, once lost or stolen, is used to make unauthorized purchases.
- Mail intercept fraud happens when fraudsters intercept cards sent through the mail to use them fraudulently.
- Mail/telephone order fraud (CNP fraud) involves using cardholder details for transactions without physically presenting the card, often through mail or phone transactions where only the card information is shared.

2.3. CNP Fraud

Card Not Present (CNP) fraud is distinct from other types of behavioral fraud because it doesn't require the physical card to be present for transactions. This type of fraud is classified as either a hybrid or output crime:

- Hybrid cybercrime involves gathering credit card details through real-world methods like skimming or scanning physical cards.
- Output cybercrime entails obtaining unauthorized credit card information via online platforms or through telephone transactions.

Essentially, CNP fraud is the culmination of a series of events, representing the final stage of a complex process rather than a single incident [4].

In 2020, Dr. Padmalatha emphasized the leading types of fraud in electronic and digital transactions [5]:

Identity theft: This type of fraud involves the unauthorized access to someone's personal information, which is then used to execute further fraudulent actions.

Friendly fraud occurs when customers deliberately purchase goods or services, complete the payment, and then file a chargeback, falsely claiming that their account was compromised. This tactic is used to secure a refund while retaining the purchased items or services.

Clean fraud occurs when a stolen card is used to make a purchase, with the transaction crafted to evade fraud detection systems entirely.

Affiliate fraud involves tricking legitimate users into visiting merchant sites through fake accounts or using automated methods to generate fraudulent traffic, often to claim commissions or rewards fraudulently.

Triangulation fraud is a scheme in which fraudsters set up a fake online storefront offering popular products at unusually low prices. Customers, attracted by the discounts, provide their credit card information and shipping details, which are then captured by the fraudsters. The fraudsters fulfill the original order by making purchases using stolen credit cards, shipping the goods to the customer to maintain the storefront's legitimacy. Meanwhile, they continue to make additional unauthorized purchases with the stolen information. This lack of a direct link between the initial and fraudulent transactions allows the scheme to evade detection for longer periods, often resulting in significant financial losses.

Merchant fraud happens when merchants advertise products at attractive, low prices but fail to deliver them after receiving payment. Customers are left without their purchases, while the fraudulent merchants profit from the payments without fulfilling orders.

The fraud types outlined by Dr. Padmalatha illustrate the most common tactics used in electronic and digital transactions to commit fraudulent activities.

3. CONVENTIONAL METHODS FOR PREVENTING FINANCIAL FRAUD

Financial institutions have historically employed diverse models to monitor the usage of cards over time, enabling them to detect any unusual activities. This proactive approach has proven effective in mitigating application fraud and cases involving stolen or lost cards. Moreover, financial institutions have implemented organizational measures, such as requiring cardholder confirmation before activating a card, resulting in a notable reduction in mail intercept fraud incidents.

Financial institutions are also urged to adhere to global security regulations and to invest comprehensively in standard tools that are widely recognized and mandated by card system schemes. Some of the prominent security measures commonly employed include:

3.1. Compliance with the guidelines and regulations of the Payment Card Industry (PCI)

Financial institutions are dedicated to aligning with the latest security standards established by the Payment Card Industry (PCI). The PCI standards include PCI DSS for secure infrastructure and **PCA DSS** for financial system software protection. This standard necessitates various measures, such as encrypted communication, prohibition of storing sensitive data, implementation of two-factor authentication, and utilization of robust password hashing algorithms [23].

3.2. Europay Mastercard Visa (EMV) Standard

The adoption of the EMV standard has greatly enhanced transaction security for chip cards. As a result, financial institutions that have transitioned from magnetic stripe cards to chip cards have experienced a substantial reduction in counterfeit card fraud. However, it is worth noting that fraudsters have shifted their focus towards casrd-not-present (CNP) fraud following the widespread adoption of EMV technology.

3.3. Card Verification Value (CVV)

The CVV2 is a three-digit security code located on the back of credit cards, providing an extra layer of security to help prevent credit card fraud by confirming the cardholder's legitimacy. However, it’s essential to recognize that CVV2 does not protect against fraud when a card is lost or stolen [8].

3.4. Address Verification Service (AVS)

Issuing banks provide merchants with the Address Verification Service (AVS), which allows them to accept or decline payments by verifying the billing address provided by the card user. However, the widespread adoption of this service is still limited, and it does not offer protection against application fraud [8].

4. SECURITY PROTOCOLS FOR E-COMMERCE

A security protocol plays a crucial role as the primary defense mechanism in preventing electronic financial fraud. In the following discussion, we will outline the various actors engaged in a security protocol, the essential security requirements it must fulfill, and provide an overview of the state-of-the-art security protocols proposed in the literature by card schemes and academics.

The security protocol typically involves four key actors: the client or cardholder, the merchant or service provider (SP), the issuer bank (providing payment services to the cardholder), and the acquirer bank (providing payment services to the merchant) [6].

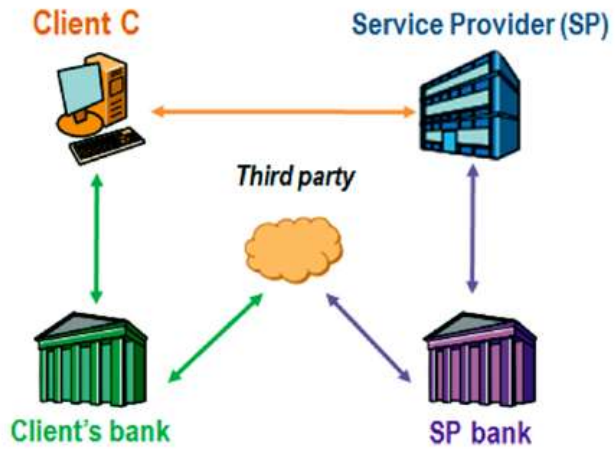

Figure 2 Security Protocol Actors

The effectiveness of a security protocol is primarily determined by critical security requirements, which meet the following criteria [9]:

Confidentiality means that all information involved in transactions must remain private. For example, if sensitive data like account numbers or usernames are accessed by unauthorized parties, they could be misused. Additionally, competitors gaining access to order and payment details could lead to lost business opportunities. Therefore, encryption is essential for securely transmitting electronic information.

Integration requires that the protocol includes mechanisms to verify data integrity, ensuring that web data remains unaltered during transmission.

Authentication of participants: Since the parties involved in a transaction may have no prior relationship, establishing their identities is crucial. Proper authentication is the foundational step in ensuring a secure and successful transaction.

Non-repudiation: the transaction should include services that prevent any party from denying their actions, such as sending order or payment details, or confirming receipt of these. This service is essential for both the consumer and the merchant to ensure accountability in the transaction process.

End-user implementation encompasses key aspects such as usability, flexibility, affordability, transaction speed, and interoperability, ensuring a smooth, accessible, and efficient experience for the end-user across various systems and platforms.

In this context, we will provide a comprehensive overview of the cutting-edge security protocols implemented in real-world electronic payment systems, along with some robust protocols proposed by academics.

4.1. Secure Socket Layer (SSL)

SSL was the first security protocol implemented in the industry specifically to secure electronic transactions. One of the main advantages of SSL is transparency. Its presence is completely invisible for merchants and cardholders. There is no cost for its integration apart from the cost of installing the certificate. For customers, SSL is widely used in web browsers to secure connections, and it requires no additional software installation for users, as it is built into most browsers. Being less complex, SSL results in minimal impact on transaction speed.

However, SSL does not enable cardholder authentication, as certificates are not mandatory and may not be directly linked to a credit card. SSL primarily protects the communication channel between the customer and the merchant, it cannot guarantee the merchant will not misuse payment information or protect them against intrusion at its server. In the absence of a third-party authority, SSL cannot ensure non-repudiation, as it does not provide mechanisms to prevent either party from denying their participation in the transaction [7].

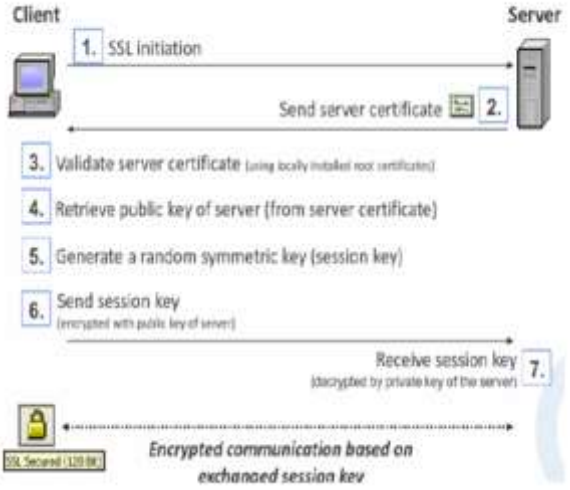

Figure 3 Overview of the SSL protocol [7]

4.2. Secure Electronic Transaction (SET)

SET (Secure Electronic Transaction) is a standardized industry protocol developed by companies such as Visa and Mastercard to secure payment transactions and authenticate all parties involved. SET ensures confidentiality, authentication, and data integrity through formalized methods. It prevents merchants from accessing customer payment information by encrypting it with the payment gateway's public certificate, and it also safeguards merchant privacy by restricting the payment gateway from viewing order details.

However, SET requires customers to install additional software and obtain a valid certificate to complete transactions. Implementing SET can be costly and complex for merchants, as it involves adapting their systems and handling intricate cryptographic methods that may impact transaction speed [7]. Eventually, SET was phased out and replaced by 3D-Secure.

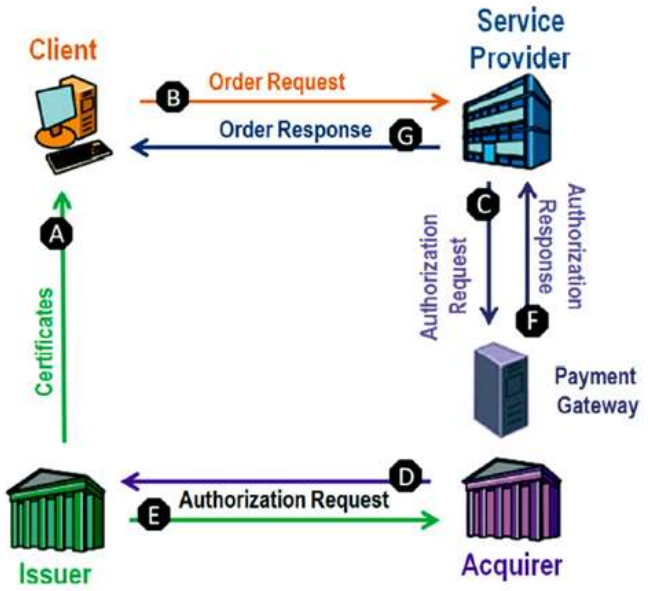

Figure 4 SET Protocol [6]

4.3. 3D Secure (3DS)

3DS is the prevailing authentication and payment architecture utilized for credit cards on the web. Originally developed by Visa in 2001 for electronic transactions, it was subsequently adopted by other major financial institutions like Mastercard and American Express. The primary objective of 3DS is to shift the responsibility of authentication from the merchant to the issuer, with the client's authentication being carried out by the issuer bank. The 3DS protocol has two versions. 3DS v1 relied on browser-based authentication, while 3DS v2 introduced application-based authentication, including support for mobile applications. In addition to some changes in message naming, 3DS v2 incorporates dynamic authentication and risk management features [6].

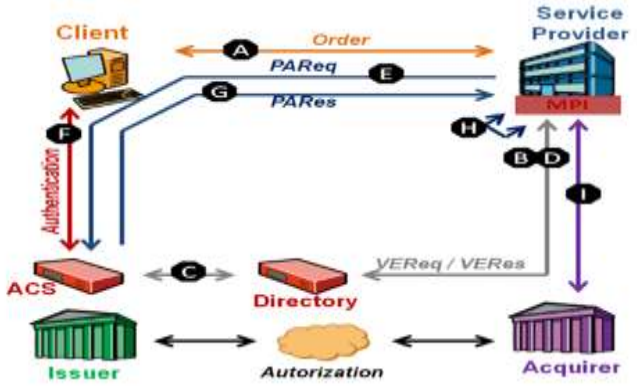

Figure 5 3D Secure Protocol [6]

5. Other Security protocol proposed in the literature

5.1. 3D Secure Improvement (3DS Imp)

Banking details such as the CVV2 code and expiration date are not essential for service providers to complete transactions. Instead, a single acquirer bank's certificate, containing standard information and the Directory public key, could suffice for authentication purposes. The client can utilize the Directory Server's public key, which is readily accessible to service providers, to secure the merchant's banking information. This setup would protect sensitive data without requiring service providers to access unnecessary details, while still enabling payment for purchases. However, these straightforward privacy measures have not been adopted or implemented in actual electronic payment systems [6].

5.2. Ashrafi and Ng's protocol (AN)

To enhance client privacy, Ashrafi and Ng proposed a protocol that divides personal information into two categories: payment information (BI) and purchase information (OI). Each type is encrypted with a separate key, designated for a specific party, as shown in the figure below. The primary limitation of this protocol is that all payment details are accessible to the card company, rather than being restricted to just the issuer bank.

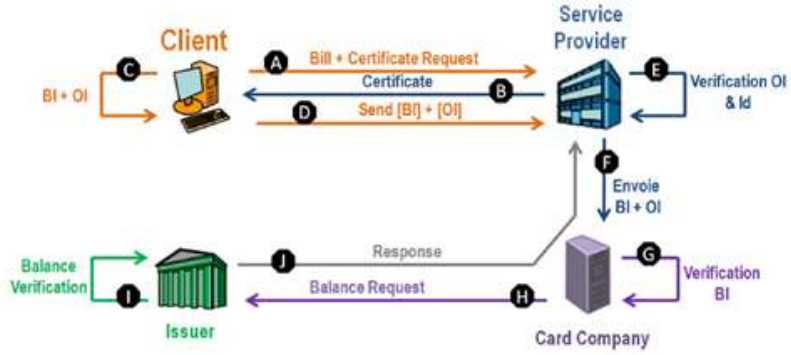

Figure 6 Ashrafi and Ng's protocol description [6]

5.3. Ashrafi and Ng's protocol Improvement (AN Imp)

An improvement to this approach involves preventing the storage of all client banking details at the card company level. Instead, verification is assigned to the issuer bank, which already has access to the necessary banking information. In this setup, the card company merely acts as a relay, reducing the frequency and extent of client data audits [6].

5.4. PLVCMR

In 2018, A. Plateaux introduced PLVCMR, a protocol developed to address the limitations of prior approaches to data security and privacy. PLVCMR operates by generating two key documents: a contract between the service provider (SP) and the client, and a bank document known as a cheque. Its architecture incorporates an interbank system that ensures only pertinent information is disclosed to the relevant parties within the transaction network [6].

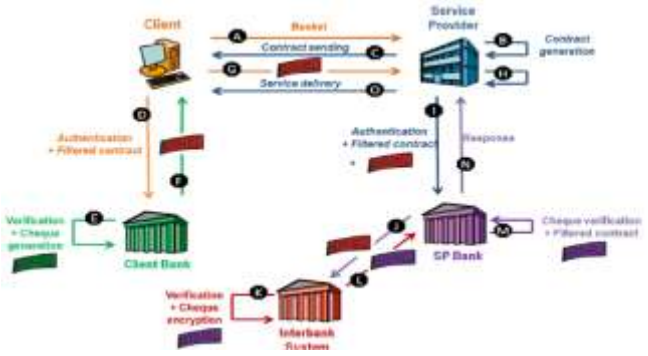

Figure 7 PLVCMR Protocol Overview [6]

5.5. Secure Electronic Transaction Payment Protocol (SEP)

The Secure Electronic Payment (SEP) protocol was introduced by Houssam El Ismaili in 2014 to provide a more streamlined approach to online transaction security. SEP is designed specifically for issuing banks, enabling cardholders to authenticate themselves without requiring third-party authentication services such as Visa or Mastercard, which are used in protocols like 3D Secure (3DS).

The SEP architecture includes an interbank component at the end of the transaction process, ensuring that only the necessary information is disclosed to the relevant actors in the system. This protocol simplifies the complexities associated with earlier security frameworks like SET (Secure Electronic Transaction) and 3D Secure, which often required elaborate implementations that added complexity to integration and utilization.

While SEP meets fundamental security requirements such as confidentiality, integrity, authentication, and non-repudiation, its real-world security and performance are yet to be thoroughly tested. Current research points to SEP's potential for simplifying the payment process while still adhering to necessary security protocols, but further study is required to confirm its robustness and efficiency under practical conditions [8].

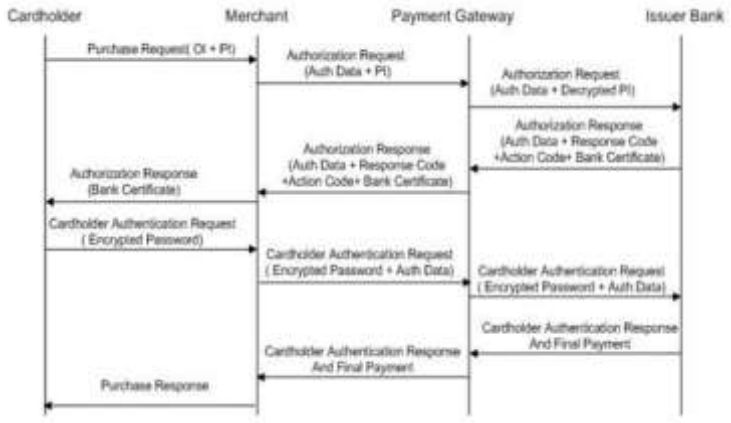

Figure 8 SEP Description [8]

5.6. iKP Payment Protocols

In 1996, Bellare introduced a protocol based on public-key cryptography, designed for implementation in both software and hardware, known as the iKP protocols. These protocols aimed to establish foundational standards for secure electronic payments:

- 1KP protocol: Only the acquirer gateway holds a public and private key pair.
- 2KP protocol: Both merchants and acquirer gateways are required to have public key pairs and certificates.
- 3KP protocol: Customers also possess a public key pair, enabling a secure, multi-party authentication system.

Each protocol stage builds on the previous, progressively enhancing security across all parties involved in electronic transactions [9].

REQUIREMENTS/PROTOCOLS	**1KP**	**2KP**	**3KP**
Issuer/Acquirer			
Proof of Transaction Authorization by Customer	+	+	++
Proof of Transaction Authorization by Merchant		++	++
Merchant			
Proof of Transaction Authorization by Acquirer	++	++	++
Proof of Transaction Authorization by Customer			++
Customer			
Unauthorized Payment is Impossible	+	+	++
Proof of Transaction Authorization by Acquirer	++	++	++
Certification and Authentication of Merchant		++	++
Receipt from Merchant		++	++

Tabel 1 Comparison of iKP Payment Protocols [9]

With (+) indicates a requirement is met but lacks robust evidence to prevent dispute and (++) signifies that the requirement is met with undeniable proof, ensuring nonrepudiation and reducing the possibility of dispute.

5.7. Secure Electronic Transaction Payment Protocol (SEP)

In 2012, Augustine Takyi introduced the Robust E-Payment Protocol (REPP) as an advanced solution aimed at overcoming the weaknesses found in previous protocols. REPP incorporates functionalities for terminating transactions and swiftly identifying errors or frauds [10].

1. **Purchase Request**: The cardholder places an order on the merchant's website (Step A).
2. **Authorization and Authentication Request**: The merchant, via the acquirer, checks if the cardholder has sufficient funds (Step B).
3. **Authorization and Authentication**: The acquirer forwards the validation request to the issuer (**Step C**)
4. **Authorization and Authentication**: The issuer confirms the purchase by prompting the cardholder to enter their password.
5. **Authorization and Authentication Response**: The issuer sends the transaction result back to the merchant through the acquirer, following the path (Steps D, C, B, A).

6. **Purchase Response:** The merchant sends a response to the cardholder (Step A)

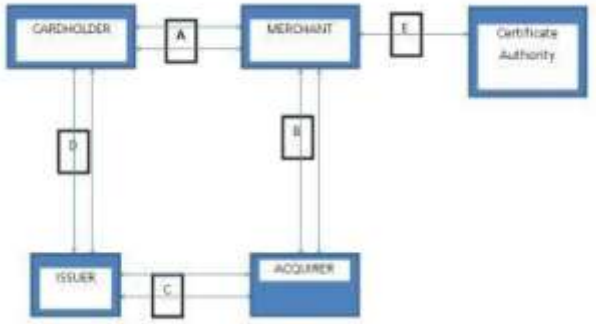

Figure 9 REEP Overview [10]
The robustness of REEP has not been demonstrated and remains a topic for future research by the author.

5.8. Comparison of security protocols for electronic payment

Protocol	Advantage	Disadvantage	Reference
SSL	Transparency: SSL operates at the session layer, making it entirely invisible to both the merchant's web shop software and the customer. This transparency is beneficial for merchants, as it requires no additional integration costs beyond the certificate installation. Ease of Use for Customers: SSL is built into most web browsers, so customers don't need to install any additional software to benefit from its security. Low Complexity: SSL's straightforward design keeps the system simple, minimizing any impact on transaction speed.	The merchant cannot reliably verify the cardholder's identity. While SSL allows for client authentication through client certificates, these certificates are optional and seldom utilized. Moreover, even if a client does have a certificate, it is not always directly associated with their credit card information.	[7] [8]

SET	Confidentiality, authentication, and data integrity in SET are verified through a comprehensive set of security proofs grounded in formal methods. In the standard protocol variant, SET ensures that merchants cannot access customer payment information, as this data is encrypted with the payment gateway's public key. Additionally, to maintain merchant privacy, SET restricts the payment gateway from viewing the order details.	To use SET, customers must install additional software capable of handling SET transactions and possess a valid digital certificate. For merchants, implementing SET is more expensive than SSL and requires a more complex system adaptation. Business banks need to either hire third-party companies to manage payment gateways or install and manage them independently. Although SET is designed with a strong focus on security, some versions of the protocol allow merchants access to customer payment information, similar to SSL. Additionally, SET uses complex cryptographic mechanisms, which can impact transaction speed.	[7] [8]
3DS v1	• Data Confidentiality and Integrity: Verified. • Bank and Client Authentication: Verified.	• SP Authentication: Not verified. • Identity Information Confidentiality for SP: Not verified. • Purchase Information Confidentiality: Not verified. • Banking Information Confidentiality: Not verified. • Acquirer Bank Confidentiality: Not verified.	[6]
3DS v1 Imp	In addition to the advantages of 3DS, banking information confidentiality is verified.	• Service provider authentication has not been verified. • Confidentiality of identity information for the service provider has not been verified. • Confidentiality of purchase information remains unverified.	[6]

		• Acquirer bank confidentiality of acquired data is not verified.	
3DS v2	• Advantages of 3DS v1 • Service provider authentication verified	• Confidentiality of identity information for the service provider has not been verified. • Confidentiality of purchase information remains unverified. • Banking information confidentiality is not verified. • Acquired bank confidentiality is not verified.	[6]
iKP	• Payment orders are authenticated using both the credit card number and PIN, along with the customer's digital signature, making the forgery of payment orders computationally infeasible. • Based on public-key cryptography, which can be implemented in either software or hardware for 3KP. • Allows merchants to authenticate customers online.	Does not prevent merchants from accessing payment details, making SET slightly more secure than 3KP.	[9]
SEP	• Ensures confidentiality, integrity, authentication, and non-repudiation. • Simplifies implementation compared to SET and 3D-Secure, making integration and usage easier.	• Static password (may incur high costs if vulnerabilities are exploited). • Special plug-ins are required to enable mutual authentication between the cardholder and merchant	[8]

	• Bypasses the complexities of 3D-Secure related to the Visa directory, potentially improving transaction speed.	(including the merchant's signature certificate and payment encryption certificate). • Transaction speed is unproven, as it depends on network speed and server performance.	
REEP	• Requires merchants to register and obtain a certificate from a trusted certificate authority, ensuring that all merchants are trustworthy. • Encrypts all data flow using SSL. • Provides the cardholder with the option to terminate the transaction. • Combines security, convenience, and ease of use.	• Robustness has not been demonstrated. • The ability of REEP to allow cardholders to terminate transactions may be unfavorable for merchants, as it could lead to abandoned carts near the end of the purchase process.	[10]
AN	• Data confidentiality is verified. • Data integrity is verified. • Service provider (SP) authentication is verified. • Bank authentication is verified. • Confidentiality of identity information for the service provider (SP) is verified. • Confidentiality of identity information for the acquirer bank is verified.	• Client authentication is only partially verified. • Confidentiality of identity information for the acquirer bank is not verified. • Purchase information confidentiality is partially verified. • Banking information confidentiality is partially verified. • Acquirer bank information confidentiality is not verified.	[6]
AN Imp	• Advantages of AN • Banking information confidentiality is verified.	• Purchase information confidentiality is partially verified. • Acquirer bank information confidentiality is not verified.	[6]
PLTCVM	Incorporates all the advantages of previous protocols while		[6]

	addressing and mitigating their disadvantages.

Table 1 Comparison of security protocol for electronic

6. AI FOR FINANCIAL FRAUD DETECTION

6.1. knowledge Discovery in (KDD process)

The KDD process, commonly used in data mining for fraud detection, follows the procedural steps outlined in [2]

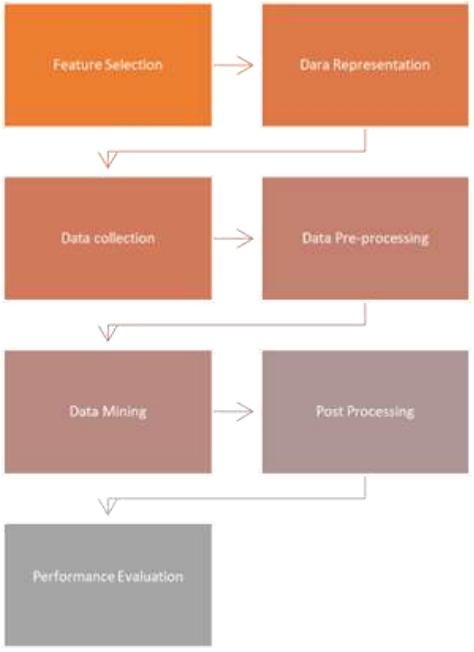

Figure 10 KDD Process

Feature Selection: The quality of data significantly influences the effectiveness of data mining applications. Data type, size, and collection frequency impact the overall data mining effort. Therefore, selecting the most suitable data is essential.

Data Representation: This stage involves choosing the internal format for gathered data, ensuring it is represented in the proper structure for analysis and storage.

Data Collection: Data is gathered from various sources and then split into training and testing sets. For financial fraud detection, data may be sourced from a mix of listed, fraudulent, and non-fraudulent firms.

Data Pre-processing: This critical step addresses inaccuracies or irrelevant data in raw datasets. Pre-processing may include handling missing data and removing irrelevant information to prepare for effective analysis.

Data Mining: Once data is collected, stored, and processed, it is analyzed using selected data mining techniques. This step uncovers meaningful patterns, transforming data into actionable information.

Post-processing: After analysis, post-processing is conducted to formally review and interpret the results obtained, ensuring clarity and alignment with initial goals.

Evaluation: A formal evaluation assesses the effectiveness and efficiency of the data mining algorithms. This review confirms how well the data mining process has met analytical objectives.

This process ensures a comprehensive approach to transforming raw data into valuable insights.

6.2. **Machine Learning (ML)**

Machine learning techniques are statistical methods generally divided into two primary categories: supervised and unsupervised learning [11].

6.2.1. **Supervised Methods**

In supervised statistical methods, estimated statistical models help distinguish between fraudulent and non-fraudulent purchase behaviors, allowing new observations to be classified into appropriate categories, such as fraudulent or non-fraudulent transactions. These supervised methods can be further divided into three categories.

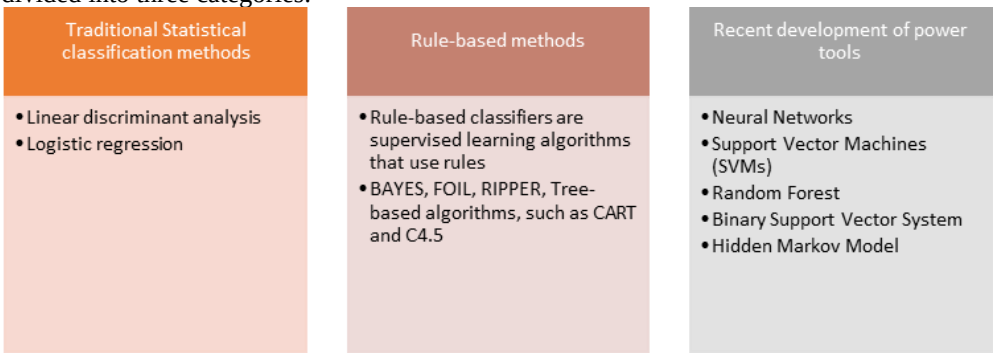

Figure 11 Supervised Methods Categories

6.2.2. **Supervised Methods**

Unsupervised methods aim to identify unusual patterns or observations, such as customers, transactions, or accounts, that deviate from typical behavior, marking them for closer scrutiny and possible classification. Unlike supervised methods, unsupervised techniques do not need pre-labeled samples of fraudulent and legitimate transactions, making them valuable in situations where there is no prior information about these classes. Additionally, unsupervised methods offer the advantage of detecting previously unknown types of fraud, whereas supervised methods are limited to identifying fraud patterns already present in historical data.k-means reaveals one of the most popular unsupervised data mining techniques.

6.3. **Standard Performance Metrics**

Following metrics are adopted to evaluate ML models.

Metric	Formula	Description
Accuracy	TN + TP/TP + FP + FN + TN	This metric evaluates the overall accuracy of the model by calculating the ratio of correct predictions—both true positives and true negatives—to the total number of samples.

Precision	TP/TP + FP	This metric reflects the proportion of predicted positive instances that are actual positives, serving as a measure of the accuracy of positive predictions.
Recall	TP / (TP + FP)	Also referred to as sensitivity or the true positive rate (TPR), recall measures the proportion of actual positive instances that the model correctly identifies.
True positive rate	TP/TP + FN	Recall, also known as sensitivity or the true positive rate, measures the proportion of actual positive instances that the model correctly identifies.
False positive rate	FP/FP+TN	This metric, known as the false positive rate (FPR), measures the proportion of actual negative instances that the model incorrectly classifies as positives.
F1-Score	2 × (Precision ×Recall)/ (Precision +Recall)	The F1 score is the harmonic mean of precision and recall, offering a single metric that balances both aspects. It is particularly useful for evaluating model performance on imbalanced datasets.
ROC Curve	Plot of TPR vs FPR	The Receiver Operating Characteristic (ROC) curve plots the true positive rate (sensitivity) against the false positive rate, providing a graphical assessment of a model's classification performance across different threshold settings.
AUC (Area Under Curve)	Integral of the ROC Curve	The Area Under the Curve (AUC) measures the area under the ROC curve, giving a single numerical value to assess the model's ability to distinguish between positive and negative instances.

Table 2 Standard Performance Metrics
With TP = True Positive, TN =True Negative, FP = False Positive, FN = False Negative

6.4. Related Search

Numerous machine learning techniques have been proposed by researchers to tackle the problem of CCF. In the upcoming paragraph, we will delve into recent studies on this topic.

In 2012, José Felipe and Adriano Pereira proposed a methodology for fraud detection in electronic transactions based on the Knowledge Discovery in Databases (KDD) process. The authors introduced a new measure called Economic Efficiency (EE), which captures the relative gains achieved by considering business rules. They defined three reference limits: Maximum Economic Efficiency (EEMax), Real Economic Efficiency (EEReal), and Minimum Economic Efficiency (EEMin). The experimental study was conducted using a real dataset from UOL PagSeguro, a major Brazilian payment system. The study employed Decision Tree (C4.5), AdaBoost, and a stacking technique that combined C4.5, RIPPER, and Naive Bayes, with Naive Bayes serving as the meta-learner in the stacking model [12].

In 2014, Evandro Caldeira and Gabriel Brandao conducted a comparative study using four techniques: Neural Networks (NN), Bayesian Networks (BN), Random Forest (RF), and Logistic Regression (LR). The results showed that Neural Networks (NN) and Bayesian Networks (BN) performed particularly well, demonstrating good results in fraud detection [13].

In 2017, Krishna Modi and Reshma Dayma concluded that Convolutional Neural Networks (CNN) were the most effective approach for fraud detection. The authors compared CNN with four other

techniques: Artificial Neural Networks (ANN), Hidden Markov Models (HMM), Decision Trees (DT), and Rule-Based Methods. To address dataset imbalance, they employed a cost sampling method for balancing the data [14].

In November 2018, Utkarsh Porwal and Smruthi Mukund proposed a method for identifying outliers and pure inliers by assigning consistency scores to each data point using the unsupervised k-means algorithm. To demonstrate the efficacy of their method, they experimented with a highly skewed real dataset from Kaggle. Instead of the traditional Receiver Operating Characteristic (ROC), the authors used the Area Under the Precision-Recall Curve (AUPRC) as the evaluation metric, as previous research indicates that AUPRC is more suitable for highly imbalanced datasets [15].

In January 2019, Chung Min Tae and Phan Duy Hung conducted experiments on seven supervised machine learning techniques for credit card fraud detection: Decision Tree (DT), Logistic Regression (LR), Naive Bayes (NB), K-nearest Neighbors (KNN), Neural Networks (NN), AdaBoost, and Random Forest (RF). They used a highly imbalanced Kaggle dataset containing 284,807 transactions, of which only 492 were fraudulent. Random Forest (RF) emerged as the top-performing technique, followed by AdaBoost [16].

In May 2019, Ying Meng and Zhaohui Zhang proposed a novel method for online transaction fraud detection based on entity relationships. The authors established a heterogeneous, sparse, and disconnected transaction network comprising entity and attribute nodes. To address this complexity, they introduced a Node Shrinkage Homogenization Algorithm to transform the heterogeneous network into a homogeneous one. Using neighborhood information aggregation and boosting tree methods, transaction attributes from neighboring nodes were aggregated through a relation matrix during the training process. When compared to models such as Logistic Regression (LR), Naive Bayes (NB), k-Nearest Neighbors (kNN), Decision Trees (DT), Random Forest (RF), and XGBoost, the proposed model demonstrated significant improvements in performance [17].

In July 2019, Anuruddha Thennakoon and Chee Bhagyani developed a real-time credit card fraud detection system using machine learning techniques. The authors worked with a highly imbalanced confidential dataset and experimented with both under-sampling and over-sampling techniques. They applied Support Vector Machine (SVM), Naive Bayes (NB), Logistic Regression (LR), and k-Nearest Neighbors (KNN) models. The results indicated that SVM, followed by LR, achieved the best accuracy [18].

In February 2020, Kristiaan Pelckmans proposed the FADO algorithm, an unsupervised machine learning technique designed for monitoring high-frequency data streams, addressing several limitations of the commonly used K-means algorithm. The author evaluated both FADO and K-means in real-time payment systems, and the results indicated that K-means with multiple clusters was unfavorable due to several factors: (1) tuning the value of K and the added complexity increased computational constraints; (2) K-means introduced variability, reducing reliability; (3) it required dimensionality reduction, which compromised the interpretability of results; and (4) the prevalence of singleton clusters further diminished reliability. As a result, FADO proved to be more favorable than K-means (with $K > 1$) in this context [19].

In January 2019, Y. Kunlin proposed a memory-enhanced framework for financial fraud detection. The framework utilized transactional logs to construct a transaction graph and embed user representation vectors. Users were clustered into groups using K-Nearest Neighbors (KNN), and the transactional logs were transformed into log vectors using the Continuous Bag-of-Words (CBOW)

model, which were then aggregated into equal-length sequences. These user groups and log sequences were input into a learner composed of a Gated Recurrent Unit (GRU) and a Memory Network to generate the final fraud score [20].

In October 2019, L. Sammani and I. Jayasooriya proposed a fraud detection solution for monetary transactions using Autoencoders. They experimented with the model on a synthetically unbalanced dataset and employed the Adaptive Synthetic Sampling (ADASYN) technique to address data imbalance. The authors demonstrated that the model could effectively classify financial transactions as fraudulent or genuine, achieving an AUC score of 83%. Additionally, the model proved capable of detecting fraudulent events in real time, outperforming traditional unsupervised machine learning approaches [21].

In August 2020, B. Branco and P. Abreu proposed a real-time credit card fraud detection approach based on the Gated Recurrent Unit (GRU) deep learning technique. Their experiments demonstrated that GRUs are more suitable for production environments than Long Short-Term Memory (LSTM) networks, as GRUs manage only one recurring state instead of two, resulting in lower computational complexity and improved efficiency [22].

In September 2020, Y. Alghofaili and A. Albattah proposed a financial fraud detection model using the Long Short-Term Memory (LSTM) deep learning technique. Compared to Random Forest (RF), Logistic Regression (LR), and Support Vector Machines (SVM), LSTM demonstrated superior performance in terms of speed, accuracy, handling complex and large datasets, and dynamically adapting to new fraud patterns. The authors also found that LSTM outperformed Autoencoders, achieving near-perfect performance in detecting fraud [23].

In 2020, I. Sadgali and N. Sael proposed an adaptive credit card fraud detection model with three security layers. The first layer, the authentication layer, acts as the initial defense by verifying user identities. The second, a behavior layer, utilizes a classical risk management module based on static rules stored in a financial institution's database to assess transaction risks. The third and most advanced layer, the smart layer, combines Bidirectional Gated Recurrent Units (BGRU) and Support Vector Machines (SVM). Transactions with normal risk scores from the behavior layer are handled by SVM, while critical scores are processed by BGRU, providing a dynamic and adaptive approach to fraud detection. This model enhances accuracy and adaptability in detecting evolving fraud patterns.

6.5. Synthesis and discussion

Based on the review of state-of-the-art ML and DL techniques, **Table 4** provides a comprehensive summary of the key methodologies and research findings in credit card fraud detection

Technique	Methodology Description	Used Metrics	Data Set	Results	Reference
C4.5 + RIP + LAC + NB + Stacking	Utilized boosting (AdaBoost), stacking techniques, and oversampling to improve performance	Precision, Recall, Economic Efficiency (EE)	Real dataset from UOL PagSeguro, Brazil	The stacking technique achieved a 46.46% gain, followed by the oversampling technique with a 36.42% gain, and Naive	[12]

				Bayes (NB) with 18.08%. While RIP demonstrated high precision and broad fraud coverage, NB outperformed it in terms of Economic Efficiency (EE), as the frauds detected by NB had higher values. Although C4.5 exhibited strong fraud coverage, its precision resulted in a lower EE compared to NB. LAC performed poorly, as it required the discretization of certain variables, leading to a loss of valuable information.	
NN + BN + RF + LR	Comparative analysis using Neural Networks (NN), Bayesian Networks (BN), Random Forest (RF), and Logistic Regression (LR).	EE, Precision, Recall	Real dataset from UOL PagSeguro, Brazil	NN and NB delivered the best results, with LR following closely. NN achieved the highest gain of 43.66%, while Random Forest (RF) was the worst-performing technique.	[13]
CNN	Compared CNN with ANN, HMM, DT, and	Not specified	Not specified	HMM are scalable and can handle large	[14]

	rule-based methods for fraud detection, focusing on balancing datasets.			volumes of data, but they are computationally expensive. ANN can process complex data effectively, but they are slow to train and require significant computational power. DT are easy to interpret, but they struggle with complex data and require refined input. Rule-based methods are simple to understand and implement, but they fail to classify new types of fraud once rules are generated. CNN offer shorter training times and help avoid model overfitting.	
K-means	Under-sampling can significantly enhance the performance of outlier detection algorithms. Isolation Forest was used as a baseline for performance validation.	Weighted similarity was used to identify outliers, evaluated by AUROC and AUPRC	A highly skewed real dataset from Kaggle with 284,807 samples, including 492 fraudulent transactions.	No prior knowledge of outliers or inliers is required. For highly skewed datasets, ROC can give a misleading performance view, while Precision-Recall curves are better suited for	[15]

				imbalanced classes. AUROC offers an incomplete picture for outlier detection. The proposed model achieved a mean AUROC of 89.37% (±0.033) and a mean AUPRC of 0.2656 (±0.0380). Isolation Forest had a higher AUROC (94.82% ±0.0029) but performed worse in AUPRC (0.2656 ±0.0303), highlighting its weaker detection of outliers compared to the proposed model.	
DT + LR + NB + KNN + NN + RF AdaBoost	Compared multiple machine learning models, using SMOTE for handling data imbalance.	Accuracy, F1 Score	A highly unbalanced Kaggle dataset with 284,807 transactions, only 492 of which are fraudulent	RF ranked highest with 98.40% accuracy and a 99.19% F1 score, while Adaboost followed with 97.09% accuracy and a 98.52% F1 score.	[16]
NIAGBDT	The Shrinkage Homogenization Algorithm was proposed to transform a	KS, accuracy rate, recall rate, F1 and AUC	Data from real-world lending operations of	The model outperformed baseline techniques, achieving 72%	[17]

	heterogeneous network into a homogeneous one. Baseline models included Logistic LR, NB, kNN, DT, RF, and XGBoost.		an insurance company	precision, 64% recall, and a 68% F1 score. It also had a high ROC value of 86%, surpassing other models that typically scored below 80%.	
SVM + NB + LR + KNN	SMOTE, under-sampling, Condensed Nearest Neighbor (CNN), and Random Under-Sampling (RUS) were applied.	Accuracy	A confidential real dataset.	Four fraud patterns were analyzed (Risky MCC, ISO Response Code, transactions over $100, and unknown web addresses). Real-time fraud detection was applied. LR, NB, and SVM models achieved accuracy rates of 74%, 83%, 72%, and 91%, respectively. SVM, followed by LR, showed the best accuracy.	[18]
FADO algorithm	Real-time experimentation was conducted with dimensionality reduction, using K-means as the baseline model.	Evaluated using recall, precision, and transactions per second.	A quasi-realistic stream of 1,000,000 transactions, including 217 international transactions, was used to detect anomalies.	FADO outperformed K-means (with K > 1), proving more reliable and robust, with nearly double the computational speed. FADO achieved a recall rate of 63.76%, precision of 0.07%, and	[19]

				processed 20,000 transactions per second. In comparison, K-means (K = 20) had a recall of 25.7% and the same precision of 0.07%. K-means struggles with multiple clusters due to tuning complexity and added variability, making it less reliable. It also requires dimensionality reduction, which compromises the interpretability of detections. The occurrence of singleton clusters further reduces its reliability.	
MermoryFraud	The GRU with Memory Network was evaluated, using SVM, DNN, Random Forest (RF), Pure GRU, and GRU + Memory as baselines.	Evaluated using recall, precision, and accuracy	A real dataset from a collaborating Chinese online banking system.	The proposed model achieved 87.4% recall, 96.8% precision, and 96.9% accuracy, outperforming traditional classifiers (SVM, DNN, LR) and sequential models (GRU). Individual memory (FraudMemory) showed only	[20]

				slight improvement over group memory (GRU+Mem). The inclusion of memory networks significantly boosted performance and robustness, particularly in handling concept drift.	
Autoencoders	ADASYN was used for dataset balancing	Evaluated using recall, precision, F1 score, and AUC	A synthetically generated dataset.	The model achieved an AUC score of 83%, with 49.81% precision, 49.91% recall, and a 49.67% F1 score.	[21]
A GRU-based model LightGBM	LSTM was used as the baseline model	Not Specified	A real dataset from major European financial institutions	The GRU-based model without profiles outperformed the LightGBM model with profiles in most metrics. LSTMs did not convincingly outperform GRU due to their complexity and multiple learnable parameters, making GRU more suitable for production environments.	[22]
LSTM	The LSTM technique was applied independently,	Evaluated using accuracy	Not Specified	The LSTM model outperformed the	[23]

	with Random Forest (RF), Logistic Regression (LR), SVM, and Autoencoder serving as baseline models.	and loss rate		Autoencoder, achieving 99.96% accuracy and a 0.21% loss rate in 405 seconds, while the Autoencoder reached only 70.27% accuracy and a 96.08% loss rate in 318 seconds. LSTM excelled in handling complex data patterns and large datasets. RF performed well with small datasets but quickly plateaued in accuracy. SVM struggled with big data and required annotated training, making it less effective for identifying new fraud patterns and lacking transparency. LR could only predict categorical results and was prone to overfitting.	
An adaptive framework combining SVM and Bidirectional Gated Recurrent Unit (BGRU).	LSTM, Bidirectional LSTM (BLSTM), and GRU were used as baseline techniques.	Evaluated using accuracy, precision, sensitivity, and AUC.	A highly imbalanced Kaggle dataset with 284,807 transactions, including 492	The proposed BGRU model achieved 97.16% accuracy, 95.98% precision, 97.82%	[8]

	fraudulent ones.	sensitivity, and 99.66% AUC, outperforming the baseline techniques.

Based on the review of state-of-the-art ML and DL techniques, credit card fraud detection is a complex problem that cannot be addressed by a single approach. The diversity of fraud types and the evolving nature of fraud patterns require a multifaceted solution.

The availability of real datasets for experimentation is limited due to the sensitivity and privacy concerns surrounding financial data. Additionally, the fixed nature of features in available datasets further restricts the flexibility of models. Fraudulent behavior is constantly evolving, making it challenging to apply traditional pattern-matching techniques. Training algorithms is also difficult due to the highly imbalanced nature of fraud datasets. Deploying models in real-time environments, particularly those requiring millisecond-level latency, adds another layer of complexity.

Our analysis revealed that SMOTE is the most widely used technique for addressing data imbalance. Supervised ML methods, particularly NB, have shown good results compared to rule-based approaches. NN and SVM also stand out, performing better than many newer tools in credit card fraud detection.

Unsupervised ML techniques have proven effective in identifying new fraud patterns, making them useful for offline processing and transaction monitoring. However, to handle the evolving nature of fraud, hybrid models combining both supervised and unsupervised methods are essential.

Despite their utility, ML techniques encounter limitations, especially when managing large and complex datasets, which has spurred a shift toward DL models. While DL techniques often yield similar results, simplicity becomes a key differentiator. Based on our findings, GRU stand out as the most efficient, requiring fewer inputs and performing well in real-time applications.

Incorporating the relationships between transaction attributes has also yielded positive results, suggesting that introducing graph theory into fraud detection could be highly beneficial. Furthermore, enhanced models that combine multiple techniques or incorporate boosting strategies can further improve accuracy and precision.

7. CONCLUSION

This comprehensive literature review provides a detailed exploration of the methods used for detecting and preventing CCF, highlighting both traditional and advanced approaches. While traditional methods like security protocols and compliance measures have significantly contributed to reducing fraud, they are not without limitations, especially in the face of rapidly evolving fraud techniques. The advent of ML and DL models offers promising alternatives with enhanced accuracy and the ability to process complex and large datasets in real-time.

However, the application of DL models in industry remains limited due to challenges like data imbalance, real-time processing requirements, and the need for greater computational resources. Our review of ML and DL techniques revealed that hybrid models, which combine various algorithms, show the most promise for improving fraud detection accuracy. Models such as RF, SVM, and CNN have

demonstrated notable success in detecting fraudulent transactions. Furthermore, deep learning techniques such as Gated Recurrent Units (GRU) and Long Short-Term Memory (LSTM) models exhibit enhanced performance in processing complex data, particularly for real-time fraud detection.

Despite the advancements in technology, the constantly changing nature of fraud necessitates continuous innovation and improvement in fraud detection methods. This review highlights the need for the integration of more sophisticated models and a greater focus on real-time deployment to keep up with evolving fraud patterns. Future research should focus on creating more robust, adaptable models and exploring the potential of deep learning techniques for large-scale industrial application. Moreover, collaboration between financial institutions and researchers can further aid in developing industry-specific solutions that are both efficient and scalable.

REFERENCES

[1] M. B. Boubker, S. Ouahabi, K. Elguemmat and A. Eddaoui, "A comprehensive Study on Credit Card Fraud Prevention and Detection," 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), Fez, Morocco, 2021, pp. 1-8, doi: 10.1109/ICDS53782.2021.9626749.

[2] A. Jain and S. Shinde, "A Comprehensive Study of Data Mining-based Financial Fraud Detection Research," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-4, doi: 10.1109/I2CT45611.2019.9033767.

[3] Jha, Sanjeev & Westland, J.. (2013). A Descriptive Study of Credit Card Fraud Pattern. Global Business Review. 14. 373-384. 10.1177/0972150913494713.

[4] Akdemir, Naci & Yenal, Serkan. (2020). CARD-NOT-PRESENT FRAUD VICTIMIZATION: A ROUTINE ACTIVITIES APPROACH TO UNDERSTAND THE RISK FACTORS. Güvenlik Bilimleri Dergisi. 9. 243-268. 10.28956/gbd.736179.

[5] N a, Dr. (2020). E-Commerce Frauds and the role of fraud Detection Tools in managing the risks associated with the frauds.

[6] Plateaux, A & Lacharme, Patrick & Vernois, Sylvain & Coquet, V & Rosenberger, Christophe. (2018). A Comparative Study of Card Not Present E-commerce Architectures with Card Schemes: What About Privacy?. Journal of Information Security and Applications. 40. 10.1016/j.jisa.2018.01.007.

[7] Kawatra, Neetu and Vijay Kumar. “Analysis of E-commerce security protocols SSL and SET.” (2012).

[8] Sadgali, Imane & Benabbou, Faouzia & Sael, Naoual. (2021). Bidirectional Gated Recurrent Unit for improving classification in credit card fraud detection. Indonesian Journal of Electrical Engineering and Computer Science. 21. 10.11591/ijeecs.v21.i3.pp%25p.

[9] El, Houssam & Houmani, Hanane & Madroumi, Hicham. (2014). A Secure Electronic Transaction Payment Protocol Design and Implementation. International Journal of Advanced Computer Science and Applications. 5. 10.14569/IJACSA.2014.050527.

[10] Bellare, Mihir & Garay, Juan & Herzberg, Amir & Krawczyk, Hugo & Steiner, Michael & Tsudik, Gene & Waidner, Michael. (1996). iKP -- A Family of Secure Electronic Payment Protocols.

[11] Gyaase, Patrick & Takyi, Augustine. (2012). Enhancing Security of Online Payments: A Conceptual Model for a Robust E-Payment Protocol for E-Commerce. 332.

[12] Júnior, José & Pereira, Adriano & Meira Jr, Wagner & Veloso, Adriano. (2012). Methodology for fraud detection in electronic transactions. 289-292. 10.1145/2382636.2382697. E. Caldeira and G. Brandao, Fraud Analysis and Prevention in e-Commerce Transactions, 978-1-4799-6953-1/14 $31.00 © 2014 IEEE

[13] K. Modi and R. Dayma, Review On Fraud Detection Methods in Credit Card Transactions, International Conference on Intelligent Computing and Control (I2C2'17)

[14] Porwal, Utkarsh & Mukund, Smruthi. (2019). Credit Card Fraud Detection in E-Commerce. 280-287. 10.1109/TrustCom/BigDataSE.2019.00045.

[15] Meng, Ying & Zhang, Zhaohui & Liu, Wenqiang & Chen, Ligong & Liu, Qiuwen & Yang, Lijun & Wang, Pengwei. (2019). A novel method based on entity relationship for online transaction fraud detection. ACM TURC '19: Proceedings of the ACM Turing Celebration Conference - China. 1-10. 10.1145/3321408.3326649.

[16] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga and N. Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning," 2019 9th International Conference on Cloud Computing, Data

Science & Engineering (Confluence), Noida, India, 2019, pp. 488-493, doi: 10.1109/CONFLUENCE.2019.8776942.

[17] Tae, Chung & Hung, Phan. (2019). Comparing ML Algorithms on Financial Fraud Detection. DSIT 2019: Proceedings of the 2019 2nd International Conference on Data Science and Information Technology. 25-29. 10.1145/3352411.3352416.

[18] Pelckmans, Kristiaan. (2020). Monitoring high-frequency data streams in FinTech: FADO versus K-means. IEEE Intelligent Systems. PP. 1-1. 10.1109/MIS.2020.2977012.

[19] Kunlin, Yang. (2018). A Memory-Enhanced Framework for Financial Fraud Detection. 871-874. 10.1109/ICMLA.2018.00140.

[20] Chandradeva, Lakshika & Jayasooriya, Isuru & Aponso, Achala. (2019). Fraud Detection Solution for Monetary Transactions with Autoencoders. 31-34. 10.1109/NITC48475.2019.9114519.

[21] Branco, Bernardo & Abreu, Pedro & Gomes, Ana & Almeida, Mariana & Ascensão, João & Bizarro, Pedro. (2020). Interleaved Sequence RNNs for Fraud Detection. 3101-3109. 10.1145/3394486.3403361.

[22] Alghofaili, Yara & Albattah, Albatul & Rassam, Murad. (2020). A Financial Fraud Detection Model Based on LSTM Deep Learning Technique A Financial Fraud Detection Model Based on LSTM Deep Learning Technique. Journal of Applied Security Research. 15. 10.1080/19361610.2020.1815491