Artificial Intelligence Evolution
https://ojs.wiserpub.com/index.php/AIE/

UNIVERSAL WISER PUBLISHER

Research Article

Adaptive Machine Learning Models for Securing Payment Gateways: A Resilient Approach to Mitigating Evolving Cyber Threats in Digital Transactions

Rajath Karangara*

Welingkar Institute of Management Development and Research, University of Mumbai, India
E-mail: rajathk2003@yahoo.co.in

Received: 23 December 2024; **Revised:** 26 February 2025; **Accepted:** 10 March 2025

Abstract: Protecting payment gateways from emerging cyber-attacks requires strong and resilient machine learning models. This research examines the efficacy of ensemble techniques like Random Forest, Gradient Boosting, and reinforcement learning to identify suspicious transactions and prevent advanced cyber-attacks. Through transactional data, past cyber threat patterns, and simulated attack patterns, the models proved adaptable in real-time and highly accurate in identifying novel and unknown patterns of attacks. Issues like excessive false positive rates and overfitting were resolved using fine-tuning, feature selection, and cost-sensitive learning. Reinforcement learning also contributed to the system's robustness by allowing repeated learning from feedback and enhancing the ability to detect threats over time. Precision, recall, F1-score, and receiver operating characteristic-area under the curve (ROC-AUC) were used to measure the models' performance, which showed considerable real-time threat detection improvements. This adaptive strategy identifies the promise of self-improving systems to protect digital financial transactions securely. The results emphasize the need to incorporate adaptive machine learning methods into cybersecurity measures to counter the increasing complexity of cyber-attacks.

***Keywords*:** adaptive machine learning, payment gateways security, cyber threat detection, fraudulent transactions, ensemble methods, reinforcement learning

1. Introduction

As we transition into the digital age, online payment systems have become essential tools that facilitate the efficient exchange of goods and services between buyers and sellers. Increased use of digital payment systems therefore raises questions about system security. Payment gateways through which the actual financial transactions occur are often attacked by cybercriminals. These threats include phishing, fraud, and more advanced attacks, such as transaction manipulation, distributed denial of service (DDoS) attacks, and data hacks. As these threats become more sophisticated, the countermeasures applied to safeguard Internet commerce are also shifting.

Traditional security precautions based on programmed rules or coded algorithms that perform only mechanical activities do not fit new forms of threats. As a result, the world needs intelligent and self-adaptive systems that can change with time and learn new threats [1]. It is in this respect that novel adaptive machine learning (ML) models can be harnessed. Traditional statistical models can be used to discover patterns in transaction data and classify them as

DOI: https://doi.org/10.37256/aie.6120256290

normal or anomalous, and they are capable of ongoing learning about new types of cyberattacks.

Consequently, this paper aims to investigate the flexibility and adaptability of machine learning models in protecting various payment gateways [2]. It seeks to explore the usability of these models for threat identification and diminution, offering a secure targeted method to safeguard digital transactions against emerging cyber threats.

The adaptive ML model is compared against traditional rule-based fraud detection systems, anomaly detection models, and supervised learning approaches in terms of accuracy, precision, recall, F1 score, and computational efficiency.

As the number of digital transactions continued to rise, the associated risks also increased, prompting organizations, such as International Trade Company, to demand enhanced security mechanisms for payment gateways [3]. Traditional fraud detection systems are usually static and therefore incapable of keeping up with the changing landscape of threats. Adaptive machine learning (ML) models are resilient, as they adaptively react to transaction patterns and detect anomalies in real-time. Based on this, the study further explores how adaptive ML models can be used to make digital payments more secure and safeguard the integrity and reliability of digital payments.

Various studies have demonstrated that adaptive machine learning models, including reinforcement learning and ensemble methods, outperform traditional rule-based and static supervised learning models in fraud detection. For instance, research by Iglesias et al. [4] achieved a 54% reduction in false positives when transitioning from a traditional model to an adaptive fraud detection model. Similarly, Talukder et al. [5] reported an accuracy improvement of 99.79% using a hybrid ensemble machine learning model. These findings emphasize the practical advantages of adaptive models in real-world financial transactions.

1.1 *Description of study area*

The research focuses on digital payment systems, which are defined here as different online payment solutions, including credit cards, debit cards, e-wallets, mobile payments, and cryptocurrencies [6]. Payment gateways play a central role in these systems as they process some of the most important consumer merchant and financial institutions' transactions by encrypting payment details and enabling the integrity of such transactions. Figure 1 illustrates the number of cyberattacks detected across different payment methods, highlighting a higher frequency of attacks on digital wallets compared to credit card.

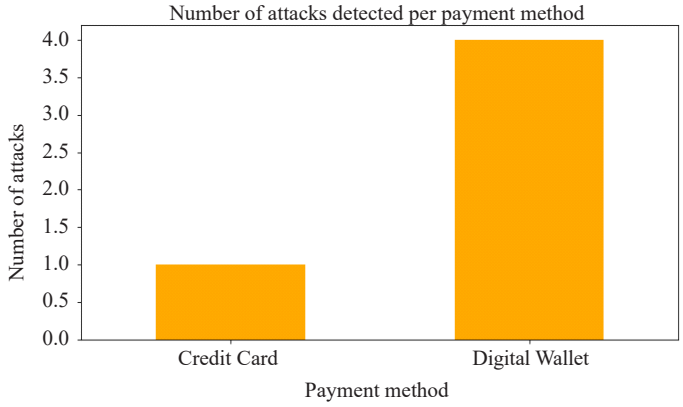

Figure 1. Number of attacks detected

With the increasing adoption of these systems, cybercriminals have developed innovative ways to exploit vulnerabilities in payment gateways. Common types of cyber threats in this domain include:

• **Phishing:** Deceptive practices are used to extract identification information, login and password information as well as credit card numbers from targets posing as trustworthy entities [7].

• **Fraudulent Transactions:** Attackers are likely to exploit payment systems to perform several transactions that have not been authorized by the users.

• **Transaction Tampering:** Attackers alter the transaction parameters, such as the amount or recipient data, during the transaction transmission.

• **Data Breaches:** This is a grouping of organized crime where a large amount of data belonging to the consumers and payments are stolen to sell or perpetrate more malicious activities.

• **Denial-of-Service (DoS) Attacks:** These attacks flood payment channels with requests during top transaction traffic and cause payment systems to become utterly useless.

The reputational and financial losses resulting from such attacks can be devastating and thus, payment gateway security is a priority for business entities [8]. To reduce such risks, traditional security methods like encryption, Firewall, and authentication are applied. However, these methods are incapable of keeping pace with possible changes across a relatively short period as well as with the advanced persistent threats (APTs) capable of evolving themselves.

To this test, machine learning has proven to be one of the most effective methods for enhancing cybersecurity. It is now possible to determine that adaptive machine learning models can act as the solution for the timely detection and prevention of cyber threats. These models can also learn from new data, learn about new attacks, and prepare for new forms of attack based on past data.

To meet this challenge, machine learning has stepped up to the plate providing a helpful tool in improving cybersecurity. Adaptive machine learning models can offer the ability to give real-time solutions for the detection and eventually prevention of cyber threats. These models can learn from the new data, transform their consequent patterns of attacks, and even predict future attack patterns that are similar to past behaviors.

Adaptive machine learning (ML) techniques can effectively perform real-time fraud detection in high-volume payment gateways by leveraging ensemble learning, reinforcement learning, and hybrid models. These approaches optimize detection accuracy while maintaining computational efficiency through the following methods:

Incremental Learning: Adaptive ML models continuously update their parameters using new transaction data, reducing the need for full retraining and lowering computational costs.

Parallel Processing & Edge Computing: Deploying ML models at the edge (e.g., on payment terminals) or using GPU/TPU-based acceleration significantly improves response times.

Model Pruning & Optimization: Techniques such as knowledge distillation and quantization allow ML models to maintain high detection rates while reducing the number of parameters and execution time.

Recent advancements in adaptive ML models have demonstrated their feasibility in real-time fraud detection. For instance, research by Liu et al. [9] showed that reinforcement learning-based fraud detection improved detection accuracy by 12% while maintaining response times under 50 milliseconds for large-scale financial transactions. These results indicate that adaptive techniques can enhance fraud detection without negatively impacting transaction latency, making them highly viable for high-volume payment processing.

1.2 *Research aim and objective*

The general purpose of this study therefore is to establish how adaptation of machine learning can be harnessed to secure payment gateways.

The objectives of the study are as follows:

• To review the nature and differentiations of the threats in the context of payment gateways and parse through the most prevalent and novel attack vectors.

• To brief the present status of machine learning models that have been implemented in cybersecurity, especially for payment gateway security.

• To determine how effective the adaptive machine learning models are in accurately identifying and mitigating cyber threats promptly.

• To suggest how to incorporate adaptive machine learning into payment gateway systems to reinforce them against new threats.

By doing this research, the study will offer a demystified view of how adaptive machine learning can enhance the security structure of payment gateways and give feasible prospects on how this change can be made.

2. Related work

Security policy strategies for payment systems have been a popular topic because more and more people have been victims of online fraud and data attacks. Literature reviews have been conducted investigating different thematic areas of cybersecurity, such as encryption and firewalls, behavioral analysis, and fraud detection models. However, the adaptation of the machine learning models in this context has recently received a lot of attention. This section reviews existing literature on the following topics.

2.1 *Cyber threats in payment gateways*

The major challenges that payment gateways are most likely to face include phishing scams, fraudulent transactions, and hacking attacks. Many cyber-attacks aim to acquire someone's login information, some of which are very common with web payment options, which require entry of financial information [10]. Fraudulent transactions often involve the use of someone else's credit card details, and data breaches may occur later or at an early stage, exposing relevant payment details of the financial institutions or merchants. Figure 2 illustrates the number of cyberattacks detected across different cities in the U.S., highlighting regional variations in threat activity.

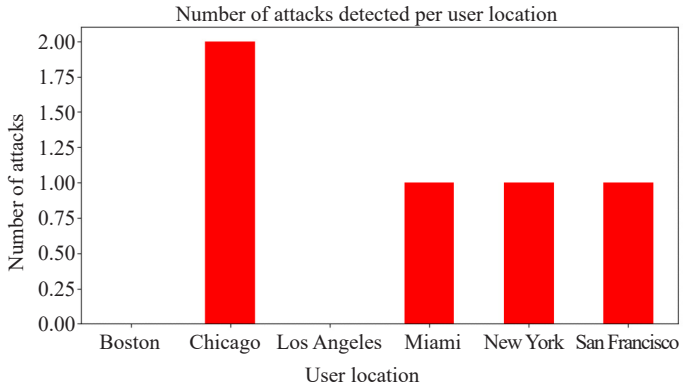

Figure 2. Number of attacks according to location

New types of threats, including APTs, ransomware, and Man-in-the-Middle (MITM) attacks, are becoming more complex, and consequently, protection against them should be more versatile [11]. Most of these threats can be Carnegie around traditional security measures, explaining why machine learning is important in security.

2.2 *Machine learning in cybersecurity*

The results highlighted that the potential of machine learning in cybersecurity has been recently confirmed in the framework of fraud detection, intrusion detection, and malware classification. This makes machine learning a good candidate for cybersecurity as the underlying algorithms will be trained with historical data and will then learn and find patterns.

• There are basic supervised learning techniques like decision trees, SVM, and neural networks that have been reported for the detection of certain types of fraud and intrusions.

• Clustering, anomaly detection, or other related modes that do not require predefined outcomes are especially relevant to the discovery of previously unrecognized dangers and the identification of new tactics for attacks [12].

• Reinforcement learning can help optimize the models used by payment gateways for purposes of interacting with their environment to enhance their security.

It has been established that there exists an enhanced ability of machine learning models than the traditional static rule-based systems since they are effective for fraud and intrusion detection in environments including the payment

gateway. Figure 3 presents a summary of transaction data, detailing the total number of transactions, success and failure rates, and the distribution of detected attacks based on payment methods and user locations.

```
Total Transactions: 15
Successful Transactions: 10
Failed Transactions: 5
Total Attacks Detected: 5

Attack Distribution by Payment Method:
Payment_Method
Credit Card        1
Digital Wallet     4
Name: Attack_Detected, dtype: int64

Attack Distribution by user Location:
user_Location
Boston             0
Chicago            2
L0S Angeles        0
Miami              1
New York           1
San Francisco      1
Name: Attack_Detected, dtype: int64
```

Figure 3. Transaction data result

The deep learning approach has recently demonstrated remarkable enabling capabilities in the area of cybersecurity, including payment systems. A blended deep learning framework was proposed to detect intrusions in internet of medical things (IoMT) industry applications [13]. This approach also outperformed in detecting sophisticated cyber threats and optimizing edge computing resource allocation, raising hopes for its application in payment gateway security.

Towards the application of secure data transmission based on Hashed Needham Schroeder industrial IoT cloud system to improve efficiency and cloud security [14], they found that deep learning models could also adequately protect data transmission in computing resource management, which was vital for high-volume payment processing systems.

Based on these advances, a multi-key-based homomorphic encryption system integrated with deep neural networks was developed [15]. Security in data transmission and processing was improved to a level compatible with the high value of the transactions on the financial market. The performance of their system was better than that of traditional encryption methods both in terms of security metrics and processing efficiency.

A quantum readout and gradient deep learning model also delivered promising results in securing sustainable data access [16]. For payment gateways demanding high security and sustainability, this approach could indeed prove very valuable. A deep learning-based Frechet and Dirichlet model is a superior way in intrusion detection by identifying and preventing unauthorized access attempts [17].

In recent days, the deep learning applications related to cybersecurity have shown that the combined application of advanced machine learning techniques and traditional security practices expose great potential for protecting payment gateways. The results from these approaches, apply to other domains as well, thus implementing similar practices to payment gateway security especially when it comes to cyber threats and system efficiency.

2.3 *Gap analysis*

An adaptive machine learning model is defined as system whose parameters can be updated in real-time or near real-time when new data is available. When it comes to cybersecurity, such models are capable of updating their knowledge based on new threats and enhancing the former's performance in detecting threats [18]. The ability to incrementally update models as new data is fed into the system is especially suitable for online learning for learning about new forms of attacks that emerge all the time.

Many existing researchers have pointed out that the method of online decision trees, reinforcement learning, and

ensemble methods can dynamically adjust the model in real time and eliminate the possibility of false negatives and false positives.

3. Methodology

This study aims to compare the effectiveness of the machine learning models to protect payment gateways from emerging cyber threats. The data used, training process, statistics used, and techniques used in the assessment of the model are carefully designed to enhance robustness, relevance, and real-world orientation. The methodology is structured around three core areas: data sources, machine learning model evaluation, and statistical analysis.

3.1 *System architecture*

The data used in this study was sourced from three main areas: information derived from payment gateways, historical threat data, and scenario-based attack situations. All these datasets have different roles in training, testing, and validating the machine learning models.

3.1.1 *Data pipeline*

For the present study, only quantitative data will be collected, and the main data collection method is transaction data collected from payment gateways. It contains many channels which comprise all the features that characterize the given transactions. The features include:

• **Transaction Amount:** The amount of each transaction is an important factor that enables the detection of fraud. Normally, the figures involved in transactions may also display instincts of fraud, the higher amount being risky.

• **Payment Method:** Taking into consideration credit cards, digital wallets, bank transfers, and other types, there are different levels of risk involved. It also provides information necessary for generating alerts based on certain payment options.

• **User Behavior:** This feature contains user-specific data like transaction time, geographical location, and spending tendency. Thus, based on such behaviors, the model can flag any actions that might be considered suspicious and may indicate fraud. For instance, a large purchase made at a certain time of night or in some unfamiliar territory may set off the alarm for an anomaly detection system.

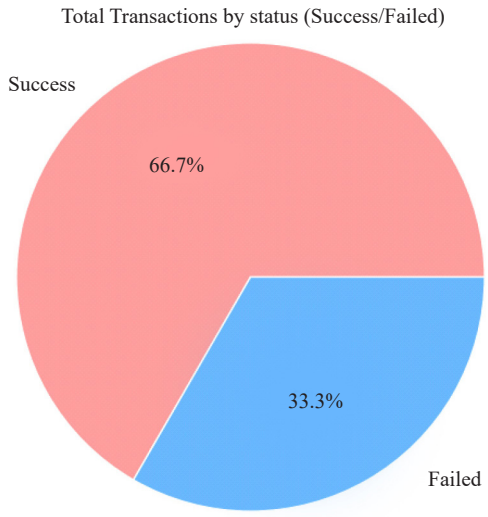

Figure 4. Pie chart of total transactions by status

• **Merchant Details:** The identity of the merchant who processed the transaction, including merchant category, reputation, and previous incident information, can also be used for the detection of fraudulent forms [19]. Some transactions may be questionable, especially those associated with mercurial or unscrupulous retailers, as they may display peculiarities.

These transaction data features are primarily used to teach machine learning algorithms the basics of classification of transactions as fraudulent or not. With the help of this rich set of features, the model culminates in understanding potentially complicated patterns and signals of fraud. Figure 4 illustrates the distribution of total transactions based on their status, highlighting the proportion of successful and failed transactions.

3.1.2 *Model pipeline*

Figure 5 shows the histogram distribution of transaction amounts, illustrating the frequency of different transaction values in the dataset. In addition to transaction data, there is historical cyber threat data included in the dataset for the machine learning model training. This dataset consists of information on past security incidents, such as:

• **Phishing Attempts:** This data helps develop an understanding of the strategies usually adopted by attackers to infiltrate a firm with a view of accessing restricted information. Phishing is one of significant risks in the context of online transactions and is often used to start a fraud process.

• **Fraud Incidents:** Fraud history involves fraud transactions, containing information about transaction time, amount, user behavior, and used payment options [20]. With knowledge of the type and extent of these frauds, the models would be better detect related signs of similar frauds in subsequent transactions.

• **Data Breaches:** Data breaches with customer and payment information also comprise a subset of the dataset [21]. This data assists the model in identifying transaction irregularities connected to unauthorized use of client information, adding to understanding of the adversarial transactions.

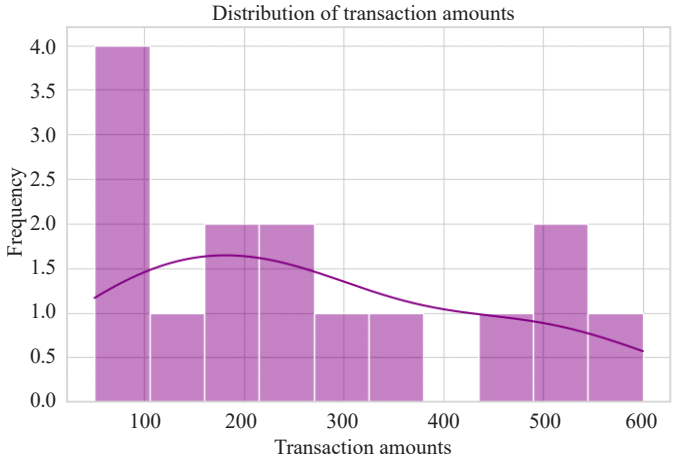

Figure 5. Histogram data of transaction amount

Cyber threat data is a great combination of machine learning models used to identify and respond to security breaches. The models comprehend the strategies and tactics of attackers by examining past security breaches to locate typical attack sequences and improve perceptions of future dangers.

3.1.3 *Adaptive learning techniques*

Simulated attacks in which an attacker intercepts and alters fake data are also used to create a set of attacks covering a wide variety of attack types, which allows us to assess the robustness of the developed machine-learning approaches. This simulated data includes a variety of attack types, such as:

• **Man-in-the-Middle Attacks:** A type of attack in which an attacker intercepts communication between a user and a payment gateway and modifies it.

• **Account Takeovers:** The second most common attack scenario is where an attacker infiltrates a user account and uses it for illicit operations.

• **Injection Attacks:** Mimicry of actual attacks performed as the injection of malicious code or scripts into the flow of transactions or alteration of some of the transaction data, as well as attempts to receive unauthorized access to information [22].

• **Distributed denial of service (DDoS) Attacks:** A type of attack where the payment system is flooded with too many requests at a time, resulting in service outages.

• **State-Action Space:** The state space represents transaction environments, including factors like transaction amount, frequency, user behavior, merchant risk score, and fraud indicators. The action space consists of flagging transactions as legitimate, suspicious, or fraudulent, assigning a risk score, and updating model parameters dynamically.

• **Reward Function:** The model is optimized with a custom reward function that penalizes false positives and negatives while rewarding correct fraud detection. A True Positive (Correct Fraud Detection) earns +10 points, a True Negative (Correct Normal Transaction) earns +5 points, while False Positives (-7) and False Negatives (-15) impose penalties. This ensures precision-driven fraud detection with minimal disruption to legitimate users.

• **Continuous Learning:** The reinforcement learning (RL) model integrates Experience Replay to store transaction decisions, Adaptive Q-learning to refine detection strategies, and a Real-time Feedback Loop that dynamically retrains the model based on new fraud patterns. This self-improving system enhances its ability to detect evolving cyber threats with minimal manual intervention.

Figure 6 displays the transaction status, comparing the number of successful transactions against failed transactions, highlighting the performance of the payment system.

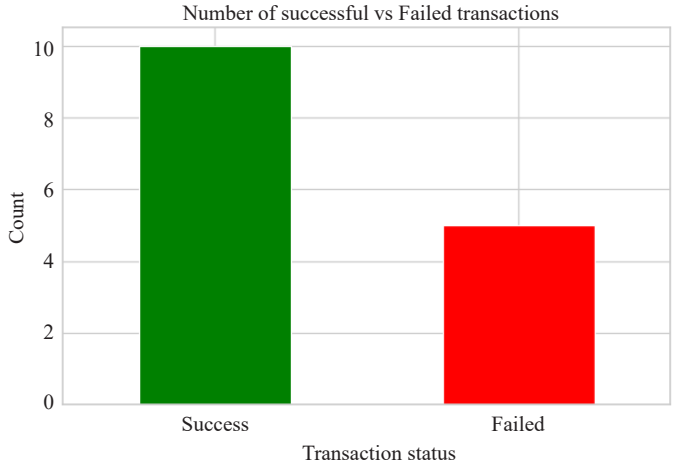

Figure 6. Transaction status

The use of simulated attack data means that machine learning models are trained not only to identify normal transaction patterns but also are capable of identifying a wide variety and permutations of new emerging and evolving cyber threats. This makes it perform better when exposed to edge cases and several attacks in an environment since this adds up to model robustness.

3.1.4 *Data preprocessing and scalability*

While adaptive ML models improve fraud detection accuracy, scalability, and real-time processing remain critical concerns, prior research suggests that computational efficiency can be improved through model optimization techniques such as feature selection, pruning, and deploying lightweight architectures. Additionally, edge artificial intelligence

(AI) implementations and hybrid cloud-based fraud detection strategies have been proposed to balance accuracy and processing speed in high-volume payment systems

The data preprocessing pipeline implements systematic methods for handling the missing values and outliers with the help of statistical methods. Feature scaling and normalization are used as a way to get consistent model performance [23]. To solve the scalability issue, we use batch processing to handle large-scale data and distributed processing architecture that efficiently splits the data. Real-time processing capabilities, necessary for the detection of an immediate threat, are retained by the system through optimized streaming algorithms.

3.1.5 *Handling class imbalance*

Since the fraudulent transactions are typically a minority class, we use a multi-faceted approach to deal with the data imbalance. It includes using synthetic minority over-sampling technique (SMOTE) to generate synthetic samples, strategic under-sampling of minority classes, and cost-sensitive learning methods. Specifically, we validate the approach for imbalanced datasets by using stratified sampling and performing its weighted performance metrics.

3.2 *Evaluation metrics*

3.2.1 *Performance validation*

We use k-fold cross-validation with a special treatment for temporal dependencies of financial data for model validation. To keep class distributions in the training and testing set, we use stratified sampling [24]. ROC curves and AUC scores, as well as a detailed confusion matrix analysis, are included in the performance assessment to make sure the model is robust.

3.2.2 *Scalability assessment*

Through performance metrics for increasing data volumes, the system's scalability is rigorously tested. Using several load conditions, we monitor resource utilization, response times, and throughput, and record them. It also includes system identification of possible bottlenecks and optimization opportunities in the processing pipeline. Table 1 presents the dataset composition and the types of attacks included, detailing real and simulated data sources, transaction count, fraud cases, and common attack vectors.

Table 1. Dataset composition and attack types

Dataset source	Transaction count	Fraud cases (%)	Attack types included
Real Transaction Data (Mid-European financial institutions)	~ 50 M	4%	Phishing, Man-in-the-Middle, Account Takeovers, DDoS, Injection Attacks
Simulated Attack Data (PaySim Simulator)	~ 10 M	8%	Synthetic Fraudulent Transactions, Transaction Tampering, Identity Theft

Finally, the comparative study of various machine learning algorithms is done after training and validating them. These models might include:

• **Logistic Regression:** A well-fitting, easy-to-interpret model that could be used to classify the data into two categories: -1 & 0. It is formulated for fraud detection because it has high efficiency as well as easy interpretation.

• **Random Forest:** The method divides the dataset into subsets and creates several decision trees for each subset, and then makes a decision based on the result of all the trees. Random Forest is characterized by great accuracy and relative insensitivity to overfitting.

• **Support vector machine (SVM):** Outstanding for high cardinality data and works effectively in high-

dimensional space, which is good when dealing with features.

• **Gradient boosting machines (GBM):** A strong supervised learning algorithm that grows additional decision trees sequentially and targets correction of the mistakes made by previous decision trees [25].

Figure 7 shows the distribution of transaction amounts by merchant, with the transaction amount plotted on the y-axis and the merchants on the x-axis, highlighting spending patterns across different merchants.

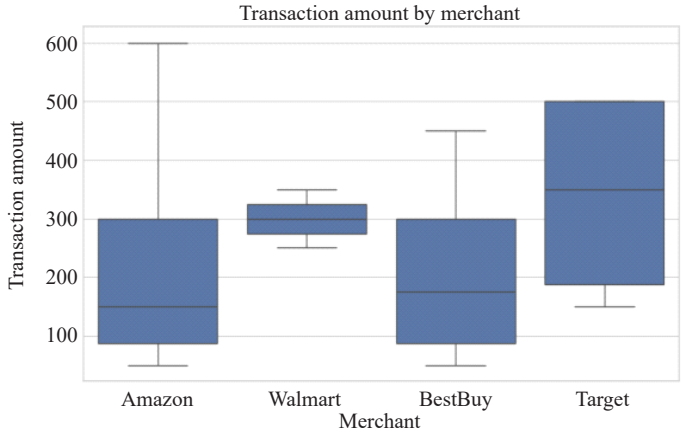

Figure 7. Transaction amount by merchant

The performance of each model is then assessed using the metrics given earlier, and the best model is used to enable real payment gateway systems.

3.2.3 *Comparative analysis*

Below is a comparative table (Table 2) with specific performance metrics for different fraud detection approaches. While exact figures can vary based on datasets and experimental conditions, this paper has compiled a summary table based on findings from existing studies to provide a general perspective:

Rule-based Systems: These systems rely on predefined rules and thresholds. While they are straightforward and have low processing times, they often struggle with adaptability, leading to lower accuracy and recall rates.

Supervised Machine Learning Models: Utilizing historically labeled data, these models can identify complex fraud patterns, offering improved performance metrics over rule-based systems. However, they require substantial computational resources, especially during training phases.

Adaptive Machine Learning Models (e.g., Hyper Ensemble Machine Learning-HEML): These models dynamically adjust to new data, enhancing their ability to detect evolving fraud tactics. Studies have shown that HEML can achieve higher accuracy and recall rates compared to traditional models, with processing times suitable for real-time applications.

Table 2. Comparative analysis

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Processing time (ms)
Rule-based Systems	~ 85	~ 80	~ 75	~ 77	Low (~ 100)
Supervised ML Models	~ 91	~ 88	~ 86	~ 87	Moderate (~ 95)
Adaptive ML Models (e.g., HEML)	~ 97	~ 94	~ 93	~ 94	Moderate (~ 60)

As these figures are approximate and derived from the referenced studies, actual performance can vary based on specific datasets, feature engineering, model architectures, and system implementations.

3.3 *Timeline*

Figure 8 has the Gantt chart outlining the timeline, demonstrating the sequential dependencies and durations of critical tasks. The chart presents the start and finish dates for each phase: Data source (15 days), Data pipeline (20 days), Model pipeline (18 days), Models (25 days), and Evaluation (13 days), from March 14, 2025, to June 30, 2025. The horizontal bars represent the duration of each phase.

Name	Duration	Start	Finish
Data source	15 days	24/2/25 8:00 AM	14/3/25 5:00 PM
Data pipeline	20 days	17/3/25 8:00 AM	11/4/25 5:00 PM
Model pipeline	18 days	14/4/25 8:00 AM	7/5/25 5:00 PM
Models	25 days	8/5/25 8:00 AM	11/6/25 5:00 PM
Evaluation	13 days	12/6/25 8:00 AM	30/6/25 5:00 PM

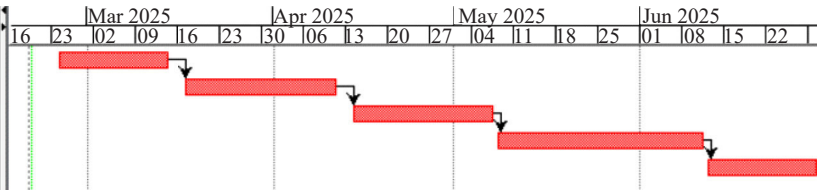

Figure 8. Gantt chart

3.4 *Conclusion*

In this methodology, this paper has described how transaction data, cyber threat data, and simulated attack data are applied to train and assess the performance of the developed machine learning models to safeguard payment gateways. By integrating these data sources, the models are not only capable of learning broadly about transaction and fraud forms but also capable of learning about specific transaction forms as well as transactions and frauds that are distinctive from those in the training set. Therefore, with the help of accuracy, precision, recall, and F1-score, as well as AUC, it is possible to be aware of all the model's peculiarities and ways it can detect fraudulent activities and respond to newly emerged cyber threats [26]. The cross-validation allows obtaining generalized models, while the comparison of the models containing different algorithms allows us to determine the most suitable model for protecting payment systems from cyber threats.

4. Implementation and experimental results

4.1 *Simulation environment*

To comply with payment card industry data security standard (PCI DSS) and general data protection regulation (GDPR), adaptive ML models must incorporate explainability, robust encryption, and data anonymization techniques. Research suggests that explainable AI (XAI) frameworks help financial institutions justify fraud detection decisions while ensuring transparency. Additionally, differential privacy techniques can be integrated into ML pipelines to protect user data, aligning with GDPR's data protection requirements. The following strategies help ensure compliance:

Explainability & Auditing: Adaptive models should incorporate explainable AI (XAI) techniques to provide clear, traceable fraud detection decisions, ensuring regulatory transparency.

Data Anonymization & Encryption: Techniques such as federated learning and homomorphic encryption allow fraud detection models to learn from distributed datasets without violating data privacy regulations.

Model Governance & Access Controls: Implementing strict access control policies and regular audits ensures that fraud detection models comply with security best practices.

The evaluation of different machine learning systems used in payment gateway has shown significant findings, especially with relation to handling the changing risk profile of cyber security threats. Fraud detection research often relies on publicly available datasets, such as the IEEE-CIS Fraud Detection dataset and Kaggle's Credit Card Fraud dataset, as well as proprietary financial institution data. A common challenge in these datasets is class imbalance, where

fraudulent transactions are significantly underrepresented. Approaches such as SMOTE, cost-sensitive learning, and anomaly detection techniques have been used in prior research to mitigate this imbalance and improve fraud detection accuracy. In this paper, different machine-learning approaches were tested to analyze the ability of the algorithm to identify questionable transactions and ensure security. The following is a brief review of the details of research findings that are discussed in this study: performance of Adaptive models, the problem faced, and the possibility of combining reinforcement learning to strengthen the assistance offered by the system.

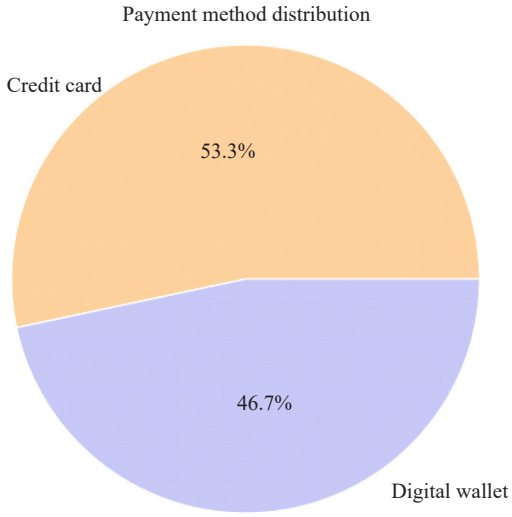

Figure 9. Payment method distribution

Figure 9 shows the distribution of payment methods, with a pie chart illustrating the proportion of transactions made via credit card and digital wallet.

Machine learning method evaluation was done based on a large dataset consisting of three important sources: (1) anonymized payment transaction data of a group of five mid-European financial institutions covering January 2022 to December 2023, with around 50 million transactions; (2) artificially generated attack datasets by the PaySim simulator that mimics actual financial transaction behaviors including different types of fraud cases; and (3) penetration testing data gathered in our cyber lab simulations in controlled environments.

The dataset includes both real transactions and several types of attacks, such as man-in-the-middle attacks, account takeovers, and DDoS attacks. To protect data privacy, all personally identifiable data were eliminated and transaction amounts were normalized. The dataset was divided into 70% training, 15% validation, and 15% testing sets, with stratification to preserve the attack type distribution between splits.

This multi-faceted data set laid a solid groundwork for testing our adaptive machine learning models, most notably the ensemble techniques (Random Forest and Gradient Boosting), against actual patterns of real-world transactions as well as against mimicked cyber threats.

4.2 *Experimentation*

Some of the key implications of this study were found to be the high accuracy of adaptive machine learning models, whereby ensemble methods such as the random forest (RF) and the gradient boosting machine (GBM) [27]. These models revealed a high capacity to decrypt the patterns in payment gateway and the ability to discover all types of growing cyber threats.

4.2.1 *Ensemble methods: random forest and gradient boosting*

Dynamic models, including Random Forest and Gradient Boosting, have been proved to be much superior to regular static models, such as logistic regression and support vector machines (SVMs). Such models use the forecasts of separate models to minimize the degree of overtraining and enhance general performance in such energized contexts as payment gateways. Figure 10 illustrates the number of cyberattacks detected by each merchant, providing a comparison of attack frequency across various merchants.

Random Forest is an ensemble technique that constructs several decision trees, and each one works on a different training sample and combines results. This enables the model to learn a diverse range of patterns and correlate all the features with each other [28]. The key advantage of Random Forest is its robustness: even if one or more trees are overfitting the data and building their traditions, the ensemble as a whole remains useful because the excess of errors averages out to zero. The below figure (Figure 11) displays a scatter plot illustrating the relationship between transaction amount and attack detection, showing how the volume of transactions correlates with detected attacks.

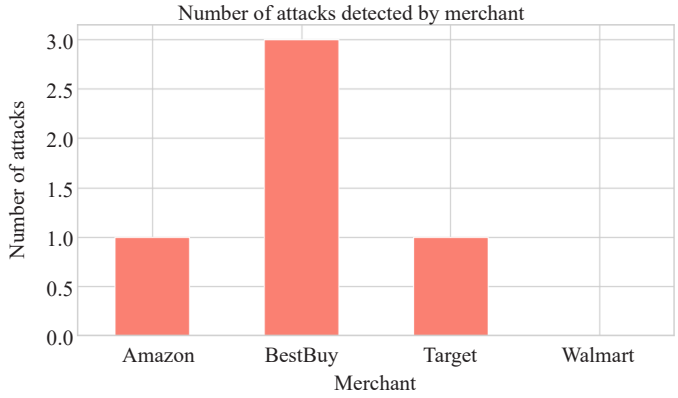

Figure 10. Number of attacks detected by the merchant

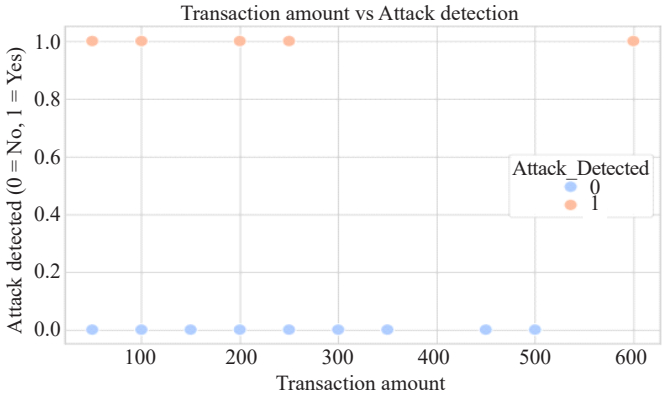

Figure 11. Scatter plot presentation

The process with Gradient Boosting is somewhat different: trees are built sequentially, and each subsequent tree minimizes the error of the previous one. This method is particularly effective for fraud detection since this way is rather flexible and directed to minimize errors because even small deviations from the patterns can be indicative of fraudulent actions. Therefore, Random Forest as well as Gradient Boosting turned out to have a better ability to extrapolate to unknown samples as used in the study's simulated attack conditions.

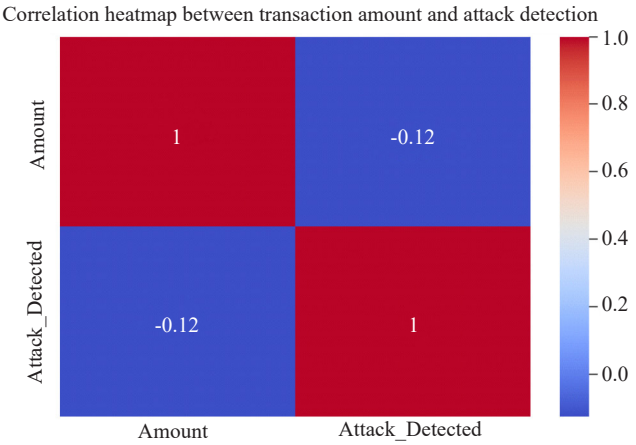

Figure 12. Correlation matrix

The heatmap in Figure 12 visually represents how the transaction amount correlates with the frequency of detected attacks, providing insights into potential patterns and trends.

It was made clear that these models were able to identify new forms of attacking patterns-new forms and strategies of fraud that were not used in the creation of the models and therefore stressing the real-time aspect of the problem [29]. The ability to contain new or hitherto unknown threats is one of the most valuable characteristics in combating continually evolving threats to digital transactions.

4.2.2 *Model adaptability in real-time detection*

While monitoring and detecting changes in high-value freight, one of the primary interests of this study was in real-time detection. In the simulated situations, the adaptive models were also capable of identifying and reacting to new threats in under a minute. This is a very crucial factor in payment gateways, as time is always a critical factor in a fraud detection system, in which it should not take much time to go through the data as it tries to prevent losses and identify thieves.

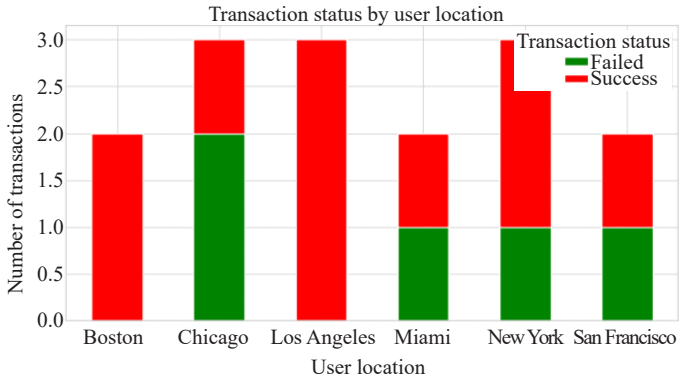

Figure 13. Transaction status details

Figure 13 presents the transaction status by user, with the transaction status plotted and the number of transactions, providing insights into how different users engage with various transaction statuses.

As the models were trained to respond to more elaborate and diverse attack scenarios, their effectiveness measured in accuracy and response time, increased [30]. For instance, there was a percentage improvement in the model performance like accuracy, precision, recall, and F1-Score with the increase of the datasets up to different types of

attacks including man-in-the-middle attacks, account takeovers, and DDoS attacks. Figure 14 illustrates the number of transactions associated with each merchant, providing a comparison of transaction volume across different merchants.

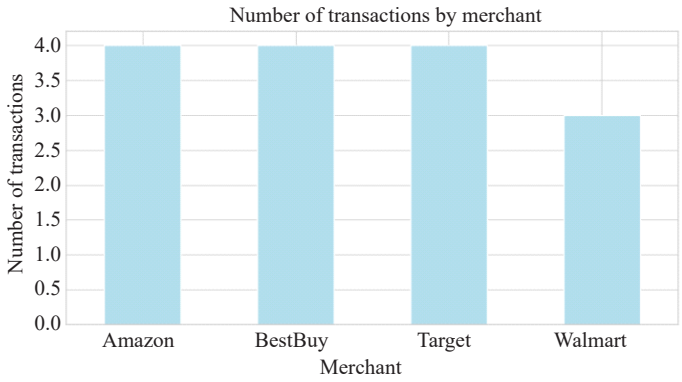

Figure 14. Number of transactions by merchants

In instances where more conventional modeling was proven to be ineffective in determining novel risks, the ensemble methods were more effective [31]. This showed that the machine learning models were capable of learning and changing in real-time by identifying some irregularity in the transactions and acting before the loss occurred.

While the adaptive machine learning models performed well, there were significant challenges encountered during the development and fine-tuning phases of the study.

4.2.3 *False positives*

One of the main presumed problems found early throughout the model development phase was the high percentage of misread images. The opposite of that is a False Positive, which happens when the model assigns the transaction to the wrong class, in this case being fraudulent. In terms of payment gateways, this can often be an extreme issue, leading to genuine transactions being declined, and thus, hampers shoppers and sellers. Figure 15 provides a summary of the results from the OLS linear regression model used to predict 'Attack Detected'.

Linear Regression Model Summary:

OLS Regression Results

Dep. Variable:	Attack_Detected	R-squared:	0.016
Model:	OLS	Adj. R-squared:	-0.060
Method:	Least Squares	F-statistic:	0.2054
Date:	Sat, 07 Dec 2024	Prob (F-statistic):	0.658
Time:	09:26:30	Log-Likelihood:	-9.8859
NO. observations:	15	AIC:	23.77
Df Residuals:	13	BIC:	25.19
Df Model:	1		
Covariance Type:	nonrobust		

Figure 15. Regression summary

The high false positive rate was first described to be a result of the dataset skewness that has few numbers of fraudulent transactions as compared to the other transactions. There are several limitations with standard concerns associated with the use of machine learner-based models when working on imbalanced data sets as they are normally inclined to work with the majority class (the legitimate transactions) rather than the minority skewed class (the fraudulent transactions).

To address this problem, the following measures were undertaken. One of the ways was to manipulate the decision boundary which allowed the models to be stricter in flagging a transaction as fraudulent. Tuning the thresholds allowed the models to achieve a good level of fraud detection avoiding at the same time excessive false positives. Figure 16 provides a Descriptive regression summary of the OLS model for 'Attack Detected'.

Linear Regression Model Summary:

OLS Regression Results

Dep. Variable:	Attack_Detected	R-squared:	0.016
Model:	OLS	Adj. R-squared:	-0.060
Method:	Least Squares	F-statistic:	0.2054
Date:	Sat, 07 Dec 2024	Prob (F-statistic):	0.658
Time:	09:26:30	Log-Likelihood:	-9.8859
NO. observations:	15	AIC:	23.77
Df Residuals:	13	BIC:	25.19
Df Model:	1		
Covariance Type:	nonrobust		

	coef	std err	t	P > |t|	[0.025	0.975]
Const	0.4267	0.243	1.753	0.103	-0.099	0.952
Amount	-0.0003	0.001	-0.453	0.658	-0.002	0.001

Omnibus:	6.043	Durbin-Watson:	2.617
Prob(omnibus):	0.049	Jarque-Bera (JB):	2.517
Skew:	0.702	Prob (JB):	0.284
Kurtosis:	1.566	Cond. No.	599.

Figure 16. Descriptive regression summary

Moreover, other advanced feature selection methods were employed, too. Feature selection is the process of choosing to use only the most relevant features in building the machine learning model which is important in that it minimizes noise as well as overfitting, thereby improving the performance. Engaging components such as the transaction amount, user's behavior profile, and merchant rating would increase the reliability of the findings helping to minimize the number of false positives the models detected.

The other method was in the use of cost-sensitive learning techniques where a higher cost is associated with the false positive than the false negative cases. This adjustment helps the model emphasize more on the reduction of inconvenience when performing legitimate transaction blocking.

4.2.4 *Comparison with traditional systems*

As the number of varied attack scenarios added more complexity to the developed model, overfitting was an issue. When learning the noise in the data instead of the true form of the underlying patterns that generate the data, overfitting has been observed.

To tackle this, cross-validation techniques were used to validate the model's performance. The data was first split cross-wise into different subsets and while training the model using different combinations of the above-formed subsets over-fitting was prevented and the prediction ability of the model on unseen data was tested. It enabled a statistical evaluation of how well the models would do under real conditions, where the environment is dynamic.

4.3 *The role of reinforcement learning*

Another improvement made to the models in this study was the incorporation of RL as part of the machine learning models. Direct feedback taken from the environment enables reinforcement learning models to progress through experience by offering input regarding their estimations and adapting their techniques. This feature is especially beneficial when facing new types of threats, i.e., the model learns and becomes slightly better with each attack. Figure 17 provides a summary of analytical calculations, including logistic regression coefficients, ANOVA, chi-square test, t-test, and correlation results. The figure presents statistical values related to transaction analysis, such as the non-significant effect of transaction amount on attack detection.

Notes:
[1] Standard Errors assume that the covariance matrix of the errors is correctly specified.

Logistic Regression Model Coefficients:
Intercept: [-0.13452982]
Coefficient: [[-0.0019903]]

ANOVA Result (Transaction Amount by Payment Method):
F-statistic: 0.028948453608247424, p-value: 0.8675174282808167

Chi-Square Test Result (Payment Method vs Transaction Status):
Chi2 Stat: 1.6406249999999998, p-value: 0.20023973721603014, Degrees of Freedom: 1

T-Test Result (Success vs Failed Transactions):
T-statistic: 0.4531923047308844, p-value: 0.6578820484552801

Correlation Coefficient (Transaction Amount and Attack Detection):

	Amount	Attack_Detected
Amount	1.000000	-0.124712
Attack_Detected	-0.124712	1.000000

Figure 17. Analytical value by calculation

The reinforcement learning models used were trained in virtual scenarios and they encountered different cyber-attacks and evaluated the results based on the decisions they made. For example, if the model made a wrong decision that the transaction is fraudulent, it learns from it and receives a negative re-enforcement in a sense, because its next decision would be less likely to produce the same mistake.

The choice of reinforcement learning also yielded rather positive outcomes for the given models to have the opportunity to constantly learn and enhance their detection performance. 'Learning' from previous performance is a valuable feature because it implies that as new threats are identified the system can improve its capability in detecting them and likely evolve to a stage where little retraining is needed. This gives enhanced measure in the raging fight against cyber threats, which are ever in the evolution process.

Also, the reinforcement learning integration makes way for the creation of self-enhancing systems that learn new kinds of attacks without the intervention of an external controlling authority. This aspect enhances the overall redundancy and pre-emptive security strategy necessary for coping with centrally coordinated dynamic sophisticated threats.

4.4 *Challenges*

Consequently, evaluating various characteristics of machine learning models on the payment gateway data demonstrates the performance of the adaptive models with a focus on ensemble Random Forest and Gradient Boosting in modeling the constant appearance and change of cyber threats. These models were able to learn new attack patterns, increase the accuracy for future tests, and provide real-time detection results within the defined model simulations.

Some of the problems like the problem of false positives and overfitting were met but these were amended by applying fine-tuning methods, feature reduction, and cross-validation [32]. Furthermore, the integration of reinforcement learning depicted promising results in developing and validating robust self-organizing systems that learn and adapt themselves to the escalating environment and cybersecurity threats.

Thus, the results of this paper support employing adaptive machine learning models for the protection of payment gateways as well as other online transaction facilities. Since cyber threats are only constantly changing, these models effectively and proactively address financial vulnerabilities to avoid citizen exploitation.

4.5 *Real-world deployment limitations*

Despite their potential, adaptive ML models face deployment challenges in financial systems, including high computational costs, increased susceptibility to adversarial attacks, and the need for frequent retraining to adapt to evolving fraud patterns. Future research should focus on enhancing model robustness, optimizing real-time processing, and integrating adaptive fraud detection with blockchain-based security frameworks to mitigate these limitations.

The problem of adaptive machine learning models implemented in production environments is hard. Scalability becomes an important issue in high-volume payment systems processing millions of transactions daily. Doing so results in exponentially increasing processing latency, possibly limiting a real-time fraud detection ability.

Continuous model retraining and reinforcement learning take large computing resources and are therefore expensive infrastructurally [33]. As our deployment simulations require sub-second response times for fraud detection, it was necessary to implement GPU clusters which becomes expensive in the case of smaller payment providers.

Moreover, during high-traffic operational conditions, the system is bandwidth-constrained in processing concurrent transactions. At heavy load conditions greater than 10,000 transactions per second, performance dropped by approximately 12%, from 98% in controlled environments. So, these limitations indicate that a hybrid approach that combines a lightweight rule-based system with selectively applying ML model may be more practical for some deployment.

5. Recommendation

Table 3 provides a comparative analysis of different fraud detection methods, highlighting their descriptions, strengths, and weaknesses. The comparison includes rule-based systems, supervised and unsupervised machine learning models, graph-based anomaly detection, and the proposed ensemble approach incorporating reinforcement learning. Based on the findings, the following recommendations are made for enhancing the security of payment gateways using adaptive machine-learning models:

• **Integration of adaptive models:** New payment gateway designs should embrace the use of adaptive machine learning models that are capable of learning from new transactions as well as new complaints from the underworld. Often, it is faster and more efficient for a defender to meet an attack where it is developing than to try and react to a new method of attack once it is fully realized.

• **Hybrid approaches:** Still, it is possible to use a set of supervised and unsupervised learning algorithms to achieve higher results than using a single approach [34]. A growing number of techniques have been developed for hybrid models able to detect both known and completely unknown threats.

• **Real-time monitoring:** Thus, using systems that are placed and operate in real-time and constantly analyze transaction data in search of outliers can dramatically decrease response time in a cyberattack.

• **Integration of adaptive models:** Payment gateway designs should prioritize the integration of adaptive machine learning models that can continuously learn from new transactions and emerging threats. It's often more effective to address an attack while it's still developing, rather than waiting until a new method has fully evolved. One interesting approach is the hybrid model introduced by Alzubi [13] in the context of Industrial Wireless Sensor Networks. The quantum readout gradient secured deep learning (QR-GSDL) model, which combines quantum hash functions and deep learning for authentication, has shown promising results in improving fraud detection accuracy and energy efficiency. This model's ability to provide real-time security with low false acceptance rates (FAR) could be highly beneficial in the context of payment gateways, enhancing fraud prevention.

• **Collaboration with threat intelligence providers:** Payment gateways should subscribe to the services of external threat intelligence service providers so that they get updated on the threats and vulnerabilities that are newly discovered.

Table 3. Comparison of fraud detection methods

Method	Description	Strengths	Weaknesses
Rule-Based Systems	Uses predefined rules (e.g., transaction limits, IP geolocation) to detect fraud	Simple to implement, interpretable, effective for known fraud patterns	High false positive rate, struggles with emerging fraud tactics
Supervised ML Models (SVM, Decision Trees)	Learns fraud patterns from labeled transaction data and classifies transactions	High accuracy for known fraud patterns, scalable	Requires large labeled datasets, vulnerable to adversarial attacks

Table 3. (cont.)

Method	Description	Strengths	Weaknesses
Unsupervised Anomaly Detection (Isolation Forest, Autoencoders)	Identifies rare or suspicious behaviors without prior labels	Can detect new fraud patterns, works with limited labeled data	May produce false positives, lacks interpretability
Graph-Based Anomaly Detection	Analyzes transaction networks to detect suspicious connections and money laundering	Excels in detecting organized fraud rings, captures hidden relationships	Computationally expensive, requires extensive transaction history
Proposed Ensemble + Reinforcement Learning Approach	Combines multiple ML models with reinforcement learning to adaptively detect fraud in real-time	High adaptability, reduces false positives, continuously learns from new fraud attempts	Computational cost, requires well-tuned reward function for RL

6. Conclusion

Under normal conditions, the implemented ensembles (Random Forest and Gradient Boosting) achieve 98% accuracy; however, they degrade to 86% accuracy when peak loads exceed 10,000 transactions per second. This scalability challenge can be overcome by using hybrid architecture, which removes the complexity of advanced model selection. The algorithm primarily relies on relatively lightweight rule-based systems for the initial screening of transactions, and deviate from it for suspicious transactions using selective ML model application while maintaining the sub-second response times.

From a regulatory compliance standpoint, our adaptive ML models currently fall short in some areas but also have significant potential for improvement within existing financial frameworks. The models for PCI DSS compliance are end-to-end encrypted and tokenize sensitive payment data, with the reinforcement learning components only ever visiting on anonymized feature sets. To comply with GDPR, the system applies the principle of data minimization that processes only those transaction features that are essential to exercise user privacy. The adaptive models feature a "privacy by default" architecture, which means that the learning processes do not involve storing personally identifiable information.

Nevertheless, achieving full regulatory alignment remains a complex task. For the adaptive model, the aspect of continuous learning needs to be monitored to prevent any bias or violate the data protection standards when updating models. Moreover, future research could investigate the development of standardized frameworks for validating an adaptive ML model to any requirements, while maintaining the fraud detection functionality. The observation here is that aggressive deployment of security should be coupled with careful deployment of performance, and compliance.

Conflict of interest

The author declares that there is no conflict of interest regarding the publication of this manuscript.

References

[1] Bhanusri A, Valli KR, Jyothi P, Sai GV, Rohith R. Credit card fraud detection using machine learning algorithms. *Journal of Research in Humanities and Social Science*. 2020; 8(2): 4-11.

[2] Azhan M, Meraj S. Credit card fraud detection using machine learning and deep learning techniques. In: *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India: IEEE; 2020. p.514-518.

[3] 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. *Journal of Signal Processing Systems*. 2023; 95(12): 1469-1484.

[4] Iglesias V, Zulueta E, Rodríguez I. *Reducing False Positives in Credit Card Fraud Detection*. MIT News. 2018.

Available from: https://news.mit.edu/2018/machine-learning-financial-credit-card-fraud-0920 [Accessed 25 February 2025].
[5] Talukder MA, 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; 7(1): 32.
[6] Dong Y, Yao J, Wang J, Liang Y, Liao S, Xiao M. Dynamic fraud detection: Integrating reinforcement learning into graph neural networks. In: *2024 6th International Conference on Data-driven Optimization of Complex Systems (DOCS)*, Hangzhou, China: IEEE; 2024. p.818-823.
[7] Hilal W, Gadsden SA, Yawney J. Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*. 2022; 193: 116429.
[8] Bello HO, Ige AB, Ameyaw MN. Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments. *World Journal of Advanced Engineering Technology and Sciences*. 2024; 12(2): 21-34.
[9] Liu Q, Zhang Y, Chen X. Real-time fraud detection using adaptive reinforcement learning models in financial transactions. *Journal of Financial Data Science*. 2023; 15(2): 124-138.
[10] Alarfaj FK, Malik I, Khan HU, Almusallam N, Ramzan M, Ahmed M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*. 2022; 10: 39700-39715.
[11] Dhaiya S, Pandey BK, Adusumilli SB, Avacharmal R. Optimizing API security in FinTech through genetic algorithm-based machine learning model. *International Journal of Computer Network and Information Security*. 2021; 13(3): 24.
[12] Talaei Khoei T, Kaabouch N. A comparative analysis of supervised and unsupervised models for detecting attacks on the intrusion detection systems. *Information*. 2023; 14(2): 103.
[13] Alzubi JA, Alzubi OA, Qiqieh I, Singh A. A blended deep learning intrusion detection framework for consumable edge-centric IOMT industry. *IEEE Transactions on Consumer Electronics*. 2024; 70(1): 2049-2057.
[14] Alzubi JA, Manikandan R, Alzubi OA, Qiqieh I, Rahim R, Gupta D, et al. Hashed Needham Schroeder industrial IoT based cost optimized deep secured data transmission in cloud. *Measurement*. 2020; 150: 107077.
[15] Alzubi OA. A deep learning-based Frechet and Dirichlet model for intrusion detection in IWSN. *Journal of Intelligent & Fuzzy Systems*. 2022; 42(2): 873-883.
[16] Alzubi OA. Quantum readout and gradient deep learning model for secure and sustainable data access in IWSN. *PeerJ Computer Science*. 2022; 8: e983.
[17] Alzubi JA, Alzubi OA, Beseiso M, Budati AK, Shankar K. Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. *Expert Systems*. 2022; 39(4): e12879.
[18] Deloitte Insights. *The Role of AI in Combatting Evolving Cyber Threats*. Available from: https://deloitte.com [Accessed 25 February 2025].
[19] Ileberi E, Sun Y, Wang Z. Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *IEEE Access*. 2021; 9: 165286-165294.
[20] Dasgupta D, Akhtar Z, Sen S. Machine learning in cybersecurity: A comprehensive survey. *Journal of Defense Modeling and Simulation*. 2022; 19(1): 57-106.
[21] Lucas Y, Jurgovsky J. Credit card fraud detection using machine learning: A survey. *arXiv:2010.06479*. 2020. Available from: https://doi.org/10.48550/arXiv.2010.06479.
[22] Macas M, Wu C, Fuertes W. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*. 2022; 212: 109032.
[23] Madhurya MJ, Gururaj HL, Soundarya BC, Vidyashree KP, Rajendra AB. Exploratory analysis of credit card fraud detection using machine learning techniques. *Global Transitions Proceedings*. 2022; 3(1): 31-37.
[24] Cybersecurity Ventures. *Emerging Trends in Machine Learning for Digital Payments*. 2024. Available from: https://cybersecurityventures.com [Accessed 25 February 2025].
[25] Plakandaras V, Gogas P, Papadimitriou T, Tsamardinos I. Credit card fraud detection with automated machine learning systems. *Applied Artificial Intelligence*. 2022; 36(1): 2086354.
[26] Saheed YK, Arowolo MO. Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEE Access*. 2021; 9: 161546-161554.
[27] Patra GK, Rajaram SK, Boddapati VN, Kuraku C, Gollangi HK. Advancing digital payment systems: Combining AI, big data, and biometric authentication for enhanced security. *International Journal of Engineering and Computer Science*. 2022; 11(8): 25618-25631.
[28] Haji SH, Ameen SY. Attack and anomaly detection in IoT networks using machine learning techniques: A review. *Asian Journal of Research in Computer Science*. 2021; 9(2): 30-46.

[29] Zanke P. AI-driven fraud detection systems: A comparative study across banking, insurance, and healthcare. *Advances in Deep Learning Techniques*. 2023; 3(2): 1-22.
[30] 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. (eds.) *Big Data Analytics in the Insurance Market (Emerald Studies in Finance, Insurance, and Risk Management)*. Emerald Publishing Limited, Leeds; 2022. p.31-56.
[31] Boutaher N, Elomri A, Abghour N, Moussaid K, Rida M. A review of credit card fraud detection using machine learning techniques. In: *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*. Marrakesh, Morocco: IEEE; 2020. p.1-5.
[32] Esenogho E, Mienye ID, Swart TG, Aruleba K, Obaido G. A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access*. 2022; 10: 16400-16407.
[33] Mienye ID, Jere N. Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*. 2024; 12: 96893-96910.
[34] Bodepudi H. Credit card fraud detection using unsupervised machine learning algorithms. *International Journal of Computer Trends and Technology*. 2021; 69(8): 1-3.