IJEMS The International Journal for Engineering and Modern Science
Year: 2025 Volume: 4 Article ID: **25001**

A Prototype for Credit Card Fraud Detection System

Moshira A. Ebrahim[1, *], Walid Ghonim[2], Ayman H. Abd El-Aziem[2]

[1] *Computer Engineering and Information Technology Department, Modern Academy for Engineering and Technology, Cairo, Egypt*
[2] *Faculty of Computer Science and Information Systems, 6 October University, Egypt*

ARTICLE INFO.

Article history:
Received: 18-9-2024
Revised: 14-12-2024
Accepted: 14-12-2024
Available online: 16-12-2024

Keywords:

Support vector machines
Real-time data processing
Machine learning
Big data analytics
Fraud detection

ABSTRACT

Advancements in analytics are significantly changing the credit card industry, making it essential to maintain consumer trust and ensure the security of digital transactions. As credit card transactions continue to develop, advancements in fraud detection and risk assessment are vital for improving the security and reliability of financial systems. Effective fraud detection is crucial for preventing common types of credit card fraud, such as unauthorized use of virtual terminals or postal orders.

This study explores various methods for detecting credit card fraud, analyzing the pros and cons of each approach. It emphasizes the importance of accurate credit risk assessment for financial institutions to predict defaults and minimize potential losses. The study introduces new evaluation criteria that look for recurring patterns in data, assessing decision trees with support vector machines (SVMs) for fraud detection. This innovative approach effectively addresses the cold-start problem while tackling data imbalance and a variety of issues, achieving performance levels comparable to leading models.

The SPEED project is a proactive initiative that uses event-driven strategies to seize opportunities and foresee challenges. Its machine learning feature adapts to evolving fraudulent tactics, quickly identifying fraud patterns. The system's user-friendly interface aids fraud analysts in making informed decisions based on automated processes.

1. Introduction

Credit card fraud is a big issue since it accounts for between ten and fifteen percent of all fraud cases in online shopping. Better detection methods are required since fraud cases in the US typically result in losses of about 2 million [1]. A range of transaction types and unbalanced data provide challenges for researchers. Because fraudulent transactions are less common than legitimate ones, there is an unequal distribution of data, which lowers machine learning's effectiveness. The most advanced methods of fraud detection match the user's history of approved transactions with the most current transactions. This approach is simple, but it might go wrong because of the diversity of the data.

To improve detection, systems need to leverage transaction information as much as possible. However, other methods, like Random Forests [2], could find this complexity too much to bear.

This study proposes a unique assessment methodology based on the transaction spectrum pattern that has been Fourier converted. This method helps to solve issues like data variety and the

*** Corresponding author**

E-mail address: *mushira.ibrahim@eng.modern-academy.edu.eg*

cold-start problem [3]while providing a new perspective on transaction data. The three main methods include defining an algorithm to identify transactions as genuine or fraudulent, gathering time series data for Fourier processing, and comparing the spectral pattern of current transactions with those of previous legitimate transactions[4].

Considering social, economic, and political shifts, companies are requiring faster fraud detection—ideally, less than 25 milliseconds—and even predictive fraud detection. Analyzing massive amounts of historical data and data from worldwide data streams is necessary for effective fraud detection. Because of terminal problems, these data streams might be noisy and include inaccurate or partial information [5]. The authors collaborated with Feedzai, a SPEEDD consortium member, to create a reliable prototype. In addition to facilitating human factors evaluations through interviews and user interface testing with fraud experts, Feedzai supplied useful credit card transaction information [6].

2. Related Work

Several techniques are applied in real-world settings to identify fraud specially in financial data streams, including:

- **Static Approach:** The data stream is divided into equal-sized chunks using this procedure. A predetermined quantity of these starting blocks is used to train the model. It offers an organized approach to managing data, but it cannot adjust well to evolving trends over time.
- **Updating Approach:** In this case, the model is routinely retrained using the latest data blocks. While this method might be computationally intensive and could not fully capture long-term trends, it can help the model stay up to speed with new advancements.
- **Forgetting Approach:** With every new block, our technique changes the model by considering just current, valid transactions and all prior fraudulent ones. It aids in keeping attention to current developments but might have trouble preserving an all-encompassing perspective on historical data.

All these techniques have their drawbacks. They could struggle to handle large computing loads, tiny data samples, and precise user behavior modelling. The static technique is popular because it is easy to implement and works well in some circumstances, despite these drawbacks. To effectively prevent fraud, it's crucial to understand that no single solution is flawless and that a combination of ways is sometimes required [7].

Due to limited access to representative datasets and specialist expertise, academic research on credit card fraud control is difficult. Fraud detection was initially dependent on analysts manually creating rules. With no practical way to amend or remove them as fraud patterns became more intricate, these regulations rapidly became antiquated and ineffective as fraud strategies changed.

Machine learning has been the focus of the discipline to overcome these problems. Neural networks and other early techniques showed promise, but their lack of transparency made it difficult for analysts to comprehend how decisions were made. Random forests gained popularity because they can handle overfitting and provide some interpretability. Making insightful explanations is still difficult, though, as decision trees get more complicated [8]. The incapacity of rule-based systems to adjust to novel fraud patterns was a serious flaw. To address this, Milo and associates presented a tool that enables fraud analysts to modify pre-established rules in response to fraudulent transactions that go unnoticed. To enhance detection, this technology groups together fraudulent instances that are similar, extracts representatives, and develops new rules. Also, variational autoencoder-based fraud detection model [9] is proposed and employed to predict and

identify fraud. This model is composed of three basic layers: an encoder, a decoder, and a fraud detector element. it may train latent variable probabilistic models by maximizing the average value of the observed data. In addition, clustering-based model for transaction fraud detection is introduced [10] to dynamically decide on noisy locations throughout iterations. This model calculates a misclassification degree for each cluster and use it to determine if a misclassified sample represents a noisy point in the current iteration. It presents a flexible strategy for updating the weights of misclassified samples. Moreover, a paradigm utilizes a natural language processing technique is developed [11] for promoting financial fraud awareness across the board. The model's initial goal is accurate fraud detection and classification. An anti-fraud chatbot is then created as an instance of the model and deployed on a popular social network site, to monitor finance-fraud cases and give anti-fraud recommendations for dealing with predicted fraud situations. Furthermore, Afriyie [12] proposed decision trees-based approach to classify transactions as fraudulent or non-fraudulent by evaluating transaction amount, location, and time.

Numerous methods have been developed that utilize association rule mining [13]. Among them are techniques for obtaining profiles of proper conduct and formulating regulations to weed out deception. Rules that differentiate between fraudulent and non-fraudulent activity are created by combining expert knowledge with transaction log analysis in process mining techniques. Though fraudulent instances are far less frequent than valid ones, these systems suffer from data imbalance [14]. Promising alternatives are provided by machine learning algorithms built to handle complicated event definitions and data streams. These techniques are useful weapons in the continuous fight against credit card theft because they work well with temporal problems and dynamic data analysis [15].

3. Background

Fraud detection is an essential component of banking, security, and other businesses. Specialized fraud detection software like Actimize and SAS Fraud Management offer advanced solutions for identifying and controlling fraud. Analytics and data mining tools like TensorFlow and Apache Spark help analyze large data volumes and identify hidden patterns. Companies like Experian and LexisNexis offer fraud detection APIs for improved operations. Balancing privacy and regulatory issues with efficient detection tools is crucial for successful fraud prevention [16].

The primary goal of fraud detection system is to identify and put an end to illicit activities such as account takeovers, credit card fraud, insurance fraud, and identity theft. To solve these issues, a variety of techniques and methods are employed.

3.1 Rule-based techniques

These techniques operate using preset criteria intended to identify irregularities. To identify suspicious activity, these systems compare transactions to a set of predetermined criteria.

3.2 Statistical methods

It looks at user activity to find trends that don’t seem right. This method can spot anomalous behaviour that might be an indication of fraud by examining how users typically engage with services.

3.3 Machine learning techniques

It represents an important breakthrough in the realm of fraud detection. Here, algorithms learn from large datasets to uncover more complex and subtle fraud tendencies that may not be seen at first glance using traditional methods.

When detecting fraud, supervised methods employ past data—both fraudulent and nonfraudulent—to train models that categorize incoming transactions as either fraudulent or lawful. This technique is useful for recognizing established fraud trends since it is predicated on the idea that historical patterns will recur. However, it finds it difficult to deal with novels or developing fraud strategies that depart from accepted norms.

Conversely, an unsupervised method looks for abnormalities in fresh transactions rather than depending on labelled data. Although skilled fraudsters may craft transactions to avoid glaring irregularities, this method frequently fails to detect uncommon trends that could point to fraud [5].

3.4 Behavioral analytics methods

looks for tendencies that don’t appear correct by analyzing user activity. By looking at how users generally interact with services, this strategy can identify unusual activity that could be a sign of fraud.

3.5 Network analysis techniques

It investigates connections and exchanges between various entities to find fraudulent networks. This technique aids in comprehending the ways in which con artists cooperate or function within a network, exposing hidden linkages that may point to fraudulent operations. Fraud detection faces challenges due to evolving fraudsters and the need to balance data protection with efficient identification. It's crucial to ensure privacy standards are followed and reduce false positives. It's also essential to reduce the number of lawful actions incorrectly reported as fraud to prevent disruptions to business operations and consumer confidence. Adapting to these challenges is essential for effective fraud detection.

4. Fraud Detection Challenges

Additionally, there are some challenges should be considered in fraud detection applications, including:

- **Low Data Availability Challenge:** Researchers face challenges in dealing with limited data due to legal restrictions, privacy concerns, and regulatory compliance. The lack of real-world datasets, especially from financial institutions and e-commerce companies, makes advancement difficult and creating efficient fraud detection systems more challenging [17].
- **Non-adaptability Challenge:** The fraud detection sector faces challenges due to strict laws, limiting academic access to company data, and the potential for anonymized data to expose vulnerabilities in financial institutions and e-commerce companies [17]. The development of efficient fraud detection algorithms is more difficult and takes longer due to this lack of data.
- **Data Imbalance Challenge:** Japkowicz and Stephen argue that unbalanced data distributions in fraud detection techniques can hinder model accuracy. They propose two techniques: oversampling and under-sampling. Oversampling increases fraudulent transactions, while under-sampling reduces legal transactions. Balancing data improves model precision in transaction categorization, as oversampling increases fraudulent transactions and under-sampling decreases legal ones [18].

5. Applied Algorithms and Problem Statement

5.1 Applied Algorithms

This research uses the Discrete Fourier Transform (DFT) [19]as part of its assessment model, which moves away from standard analysis techniques and into the frequency domain." Reducing computing complexity from $O(n^2)$ to $O\ (n\ log\ n)$ is made possible by this transformation, which is incredibly helpful. To make this procedure easier, the Fast Fourier Transform (FFT) [20] breaks down the input matrix into a set of sparse factors, which allows it to calculate the DFT quickly. Handling massive datasets requires processing that is quicker and easier to handle, which is what our technique offers [15]. In parallel, Breiman's Random Forests Approach is a complex data analysis technique that works especially well for applications involving regression and classification. With the use of random selections of the data, this approach creates an ensemble of decision trees. An average of the results from these yields the final projection. The efficiency and efficacy of the assessment model are essentially increased by combining the frequency domain analysis with the Random Forests approach. This method is very successful for evaluating and identifying fraud in financial transactions because it makes use of DFT and FFT to maximize computing resources and Random Forests to give a trustworthy framework for accurate classification and regression [21].

5.2 Problem Statement

The cold-start problem occurs due to a well-developed model not having plentiful or diversified training data which is mandatory for the creation of a reliable system. In the case of fraud detection, this problem occurs when the training data doesn't cover all the relevant scenarios, like not addressing both good and bad transactions. This research tackles the issue by initially training the model using only valid transactions. This proactive approach enables the model to start detecting fraud, even without any prior information about fraudulent activities. Thus, the system is quite beneficial for fraud detection in its initial stages or management since it doesn't merely rely on observed fraudulent patterns.

6. Credit Card Fraud Detection

The increasing use of credit cards has led to a significant issue in fraud detection. Advancements in machine learning have revolutionized this problem by allowing models to learn from large datasets and identify potential fraud patterns. Deep learning, particularly, excels at processing vast amounts of data and spotting complex fraud patterns.

To glean insights from massive datasets, a variety of data mining techniques have been used, such as decision trees, neural network algorithms, and clustering techniques. Identifying abnormalities in behavior is yet [22]. There are still problems, such as dataset imbalances that might skew machine learning algorithms and evolving fraud techniques. Further advancements in fraud detection are anticipated from artificial intelligence and quantum computing, which integrate a variety of data sources, including social media and geolocation. In the field of credit card fraud detection, robust machine-learning models have largely superseded basic rule-based methods. It is expected that with continued technological advancements and targeted research, fraud detection will become considerably more successful [7].

6.1 Credit Risk Assessment

Loan risk assessment is a crucial aspect of the financial industry, especially as credit cards are increasingly used. Traditional methods, such as income, work status, and credit history, may not fully capture an individual's financial activity. Machine learning has transformed this business by allowing models to evaluate vast amounts of data and estimate default risk more accurately. Data analytics is now a key component of credit risk modelling, providing a more thorough evaluation of potential hazards. However, issues such as data privacy, potential biases in machine learning algorithms, and regulatory considerations still need to be addressed.

Credit risk assessment in the future will probably include efforts to guarantee ethical AI practices using cutting-edge technologies such as blockchain, quantum computing, and artificial intelligence. Furthermore, by integrating data from many sources—including social media, A more comprehensive view of an individual's creditworthiness may be provided via biometrics and the Internet. Credit risk evaluation has moved from static, rule-based approaches to dynamic, data-driven models. With the combination of big data technologies, machine learning, and sophisticated analytics, credit risk assessments have become much more accurate and efficient [23]. As technology advances, credit risk models will get more complex, giving financial institutions the ability to make safer and better-informed lending choices.

6.2 Machine Learning for Fraudulent Pattern Construction

Fraudulent conduct is often indicated by patterns in the relationships—based on time or other factors—between many credit card transactions. These connections can be represented using logical programming. For example, a fraud pattern called the" Big after Small" pattern indicates fraud when a large transaction occurs shortly after a small one. Specifically, this pattern could indicate fraud if a large transaction happens at time T2 while a smaller transaction happens at time T1 only a minute earlier. Depending on the kind of transaction, the cardholder's location, and their spending habits, thresholds are used to classify transactions as large or small [4].

These associations are frequently incorporated as features for the model during the data preparation step of credit card fraud management. Using techniques that may explicitly describe and rationalize these linkages to identify patterns of fraudulent activity is a further strategy. One such technique is Inductive Logic Programming (ILP) [24]. Logic programming is used by ILP to unify the representation of learned rules, domain knowledge, and training examples. An ILP algorithm's goal is to create a logical theory, or hypothesis, based on the given background knowledge, that reliably differentiates between positive (fraudulent) and negative (non-fraudulent) cases. Because noise makes perfect discrimination difficult to achieve in real life, ILP algorithms employ a variety of heuristics to choose the hypothesis that best matches the data [21].

Determining complex occurrences is another typical prerequisite for fraud detection. This means looking for patterns that indicate fraudulent conduct by examining lists of simpler events, such as transaction data. Event recognition systems handle streams of data, which adds complexity because learning from these streams requires live algorithms that can update decision models with each new piece of input instead of processing the data all at once. So, in this study, we employ OLED (Online Learning of Event Definitions) [15], an online relational learner built for creating complicated event patterns in a single pass over the training data, to manage the amount and velocity of training data in the fraud domain.

7. OLED-based Credit Fraud Detection System

The OLED credit card fraud detection system improves detection accuracy by dynamically learning from transaction data. This is a summary of how it functions. OLED takes advantage of fraud annotations supplied by human analysts as well as transaction characteristics (such as amount, card ID, and timestamp). To improve learning, it integrates prior information, including auxiliary predicates (such as temporal order and minimal number of transactions). OLED dynamically generates and refines rules to improve fraud detection by evaluating and expanding rules based on incoming data and their performance [7].

OLED system is designed to enhance fraud detection by iteratively refining rules based on precision. It uses a detailed process for rule evaluation and adjustment The overall operation strategy of OLED fraud detection system is explained in Figure 1.

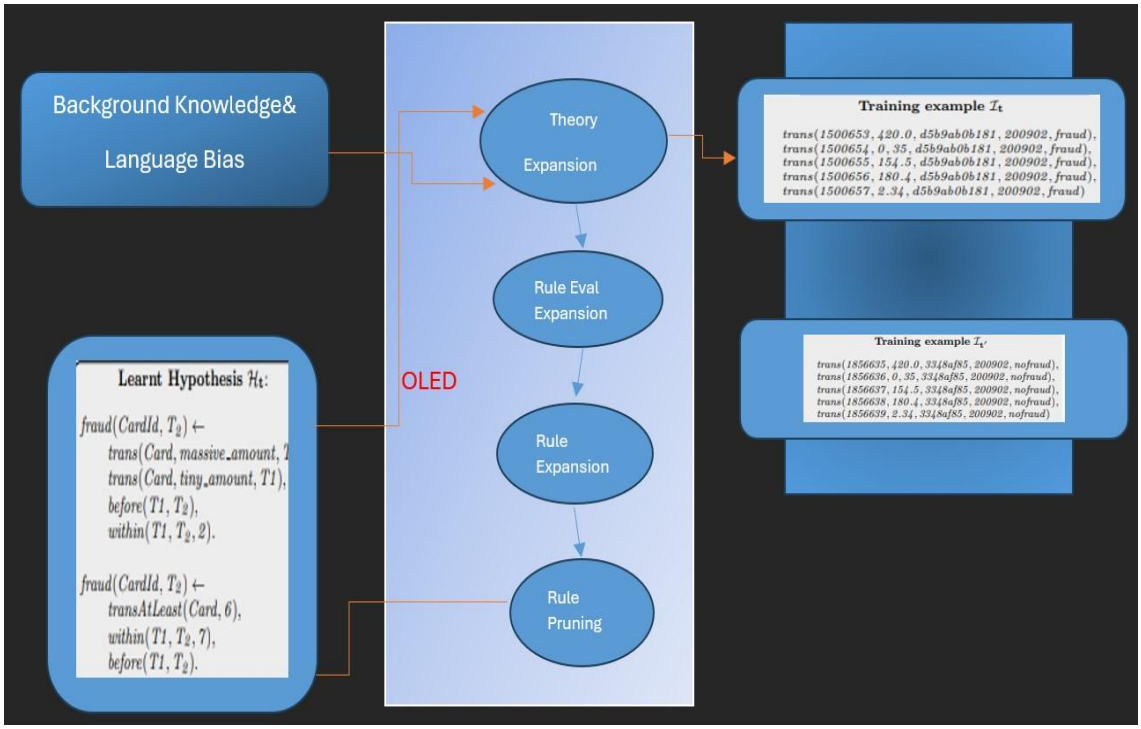

Figure 1. The OLED-based credit fraud detection system structure

7.1 OLED Input Components

- **Stream of Examples:** Includes training data with transaction attributes. Every example has a collection of transactions that were acquired by windowing, or by combining transactions that occur within a predetermined amount of time, such fifteen minutes. A minimal set of a transaction's properties, including its amount, card number, and expiration date, are shown in Figure 1 to prevent clutter.
- **Background Knowledge**: Provides definitions for auxiliary predicates used during learning.
- **Language Bias**: Defines the predicates' payloads, guiding rule formation.

7.2 Learning Process

a) **Initialization**: Begins with an empty hypothesis (H).

b) **New Data Handling:** OLED determines whether to create a new rule or improve an old one based on fresh training instances. When existing rules do not encompass positive

cases, new rules are added. Current regulations are specialized when they address many unfavorable cases.

c) **Rule Management:**

- **Theory Expansion**: Involves adding a new rule to cover specific examples. A bottom rule is created from the example and refined by combining conditions to find a rule that covers many positives and few negatives. Search Space is organized according to subsumption and directed by an assessment function (G). Either bottom rules are expanded upon, or too general rules are refined to find rules.
- **Rule Evaluation**: Each rule's performance is evaluated based on cumulative statistics from new examples. Precision is used as the evaluation metric. OLED calculates precision for each rule by counting true positives and false positives. This approach helps determine the effectiveness of each rule in classifying transactions correctly.
- **Rule Expansion**: Generates a new rule if a positive example is not covered by existing rules. OLED specializes in a rule by adding conditions from a bottom rule when it needs to be improved. To make sure that the extension of the rule is supported by a sufficient number of cases, the Hoofing bound is used, which aids in the selection of the most promising specializations. By using this approach, the rule's capacity to discern between positive and negative circumstances is enhanced [6].
- **Rule Specialization**: Refines an existing rule when it covers many negative examples.
- **Rule pruning**: Rules are specialized by adding conditions from the bottom rule. Competing specializations are evaluated, and the best-performing rule is retained. Pruning is another method used to remove conditions from a ruler's body to improve its quality. Conditions from a bottom rule are included by OLED to specialize a rule when it must be refined. Bad rules can occasionally be created that are incapable of being amended. For various reasons, OLED does not try to generalize a rule, i.e., eliminate circumstances from its body to increase its quality. It could be inefficient and unnecessary to keep these rules in the hypothesis H and to continuously assess them on fresh cases. Hoeffding bound is used for this, guaranteeing that the extension of the rule is supported by a sufficient number of cases, thereby aiding in the selection of the most promising specializations. The rule can now more accurately discriminate between positive and negative situations thanks to this strategy.

7.3 Hypothesis Output

The method makes it possible to generate the current hypothesis at every level of the learning process. Prior to a rule being considered for inclusion in the final hypothesis [25], OLED includes a" warm-up" phase that involves processing a minimum number of training samples (N_{min}). This guarantees consistency and dependable performance. Basically, OLED makes sure that the best rules are applied to detect fraudulent transactions by constantly fine-tuning its rules based on accurate assessments and adaptive modifications.

- The work is centered on online learning (OLE) and its application to transaction fraud detection. Ten thousand transactions, or about 200 MB of data, make up the dataset.
- The purpose of the first experiment was to evaluate the trade-off between output quality and efficiency. The basic offline ILP learner, which learns a rule at a time in a normal set cover loop, was contrasted with OLED, an online learning system, by the researchers [26].

- The complexity of the learning challenge grows when examples are accepted as single logical atoms by the researchers' OLED method. Using an Intel i7-4770 CPU running at 3.40GHz and 16 GB of RAM, they ran the offline ILP method and 10-fold cross-validation using OLED on a Linux system. OLED and the offline ILP method were both put into practice.
- The results showed that SC (OLED's set-cover-based offline ILP rival) functioned more accurately than OLED, although on average, SC needed more than three hours of training. OLED examined all the data in around twenty-one minutes to find patterns with comparable quality. In the second experiment, the quality of the findings in terms of the F1-score and average processing time per window was affected by adjusting the OLED window size.

8. Experimental Evaluation

Feedzai produced a synthetic dataset that resembles real credit card transaction streams to test their automated fraud pattern detecting system. Out of 10,000 transactions in the dataset, only 0.2 are deemed fraudulent. This significant mismatch increases the difficulty of learning.

To evaluate OLED, researchers compared it to a traditional offline learner using Inductive Logic Programming (ILP). OLED makes use of online education. One rule at a time, the offline ILP learner was tested with OLED using 10-fold cross-validation on a Linux workstation equipped with Intel i7-4770 CPUs and 16 GB RAM. Both approaches were implemented in Scala using the Clingo solver. This comparison is summarized in Table 1.

Table 1. Performance comparison: OLED vs online ILP

System	f1-score	Accuracy	Remember	Time (min)
OLED	0.830	0.894	0.776	21
Asus	0.892	0.912	0.874	188

The results demonstrated that whereas OLED only required twenty-one minutes of training, the offline ILP learner required more than three hours, albeit having greater accuracy.

- Mutual authentication and communication integrity are guaranteed via the ecosystem's use of badges, which function as certificates. During the first phase, these badges are only awarded to approved objects. Communications between these objects are secured by utilizing the private keys attached to the badges to sign any messages that are transmitted back and forth using the ECDSA (Elliptic Curve Digital Signature Algorithm) [27]method. This technique ensures device identity and communication integrity by using a private key only known to the object's owner. This key prevents non-repudiation and allows only the owner to sign messages, ensuring they cannot deny signing due to the exclusive nature of the key.
- The proposed method addresses scalability by utilizing a public blockchain distributed across a peer-to-peer network, which is highly effective in managing large amounts of data and transactions due to its ability to distribute load among multiple nodes.
- The proposed approach restricts each item to a single identity and key combination, preventing Sybil attacks. Each communication message must be signed using the private key associated with the unique identity, thus preventing fictitious identities.
- Spoofing attacks are avoided by ensuring that an attacker cannot mimic another item. The reason for this is that the attacker does not have the private key required for message authentication and approved object signature [28].
- Message replay prevention is achieved by treating each message as a unique transaction with a timestamp, ensuring traceability only within a specified time range. The blockchain's

consensus mechanism rejects messages outside the time window, preventing attackers from reusing or replaying previously sent messages.

- Blockchains' decentralized nature makes them resistant to denial-of-service attacks. They have multiple network nodes, ensuring other nodes continue to function even if an attacker tries to take down one. This redundancy makes it harder for attackers to take down the entire network. Additionally, financial costs and penalties associated with transactions discourage attackers from flooding the network [16].

8.1 Datasets

The proposed technique was evaluated using a real-world dataset of European credit card transactions from September 2022. With 492 fraudulent transactions out of 284,807 total, there is a significant imbalance since fraudulent transactions make up merely 0.0027 of all transactions in this sample. This extreme imbalance draws attention to the necessity for methods for handling unbalanced data and the challenge of developing effective fraud detection systems.

Correlation matrices are critical to comprehending our dataset. We want to know if there are features that influence heavily in whether a specific transaction is a fraud. However, it is important that we use the correct data frame (subsample) for us to see which features have a high positive or negative correlation about fraud transactions. Figure 2 depicts how an imbalanced dataset appears on a correlation matrix against a balanced one. When we give an unbalanced dataset to the model, it has a considerably tougher time understanding the patterns that determine the outcome of the label. On the other hand, feeding the model a balanced sample allows it to pick up patterns more effectively.

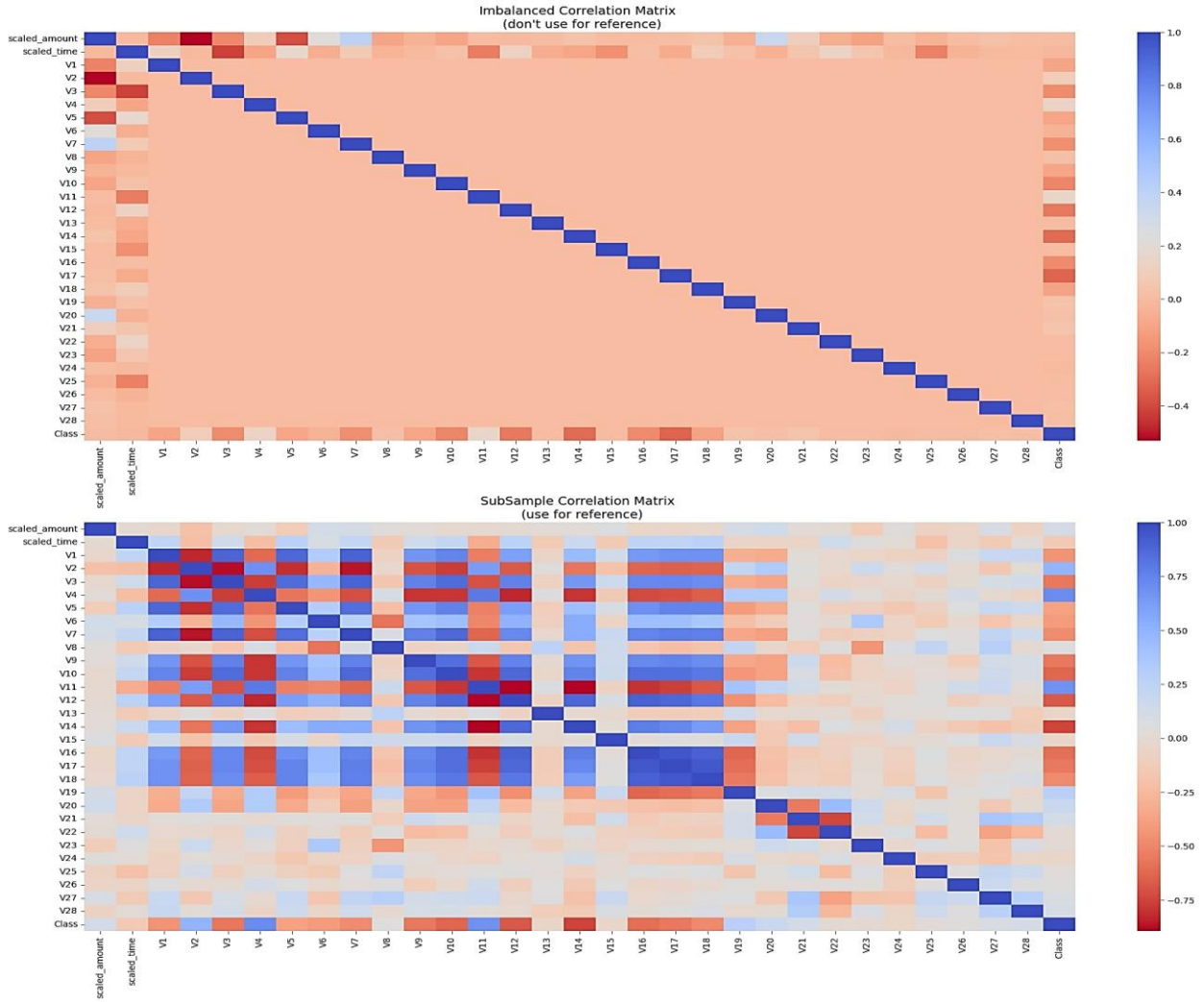

Figure 2. Correlation Matrix of our subsample data vs. imbalanced one

Within the correlation matrix. -1 represents a fully negative linear correlation between two variables. When the number is 0, it shows that there is no linear connection between two variables. While value 1 represents a fully positive linear correlation between two variables. In addition, Figure 2 shows that V10, V12, V14, and V17 are negatively connected. This indicates that the lower these numbers are, the greater the likelihood of the label being a hoax. Furthermore, V19, V11, V4, and V2 are positively connected. The higher these levels, the greater the likelihood of the label being a forgery.

Additionally, the relationship between key characteristics and target class in a fraud detection subsampled dataset is depicted in Figure 3. The top row of the figure (V17, V14, V12, V10) demonstrates the lowest correlation, with fraud occurrences having greater or negative values than non-fraud examples. While the bottom row (V11, V4, V2, V19) displays positive correlations, showing that fraud cases receive more rewards than anomalies. These findings provide insight into how attributes connect with fraud behavior, which is critical for designing and enhancing fraud detection algorithms. The distinction between Class 1 and Class 0 variables reflects their primary importance in fraud performance identification systems.

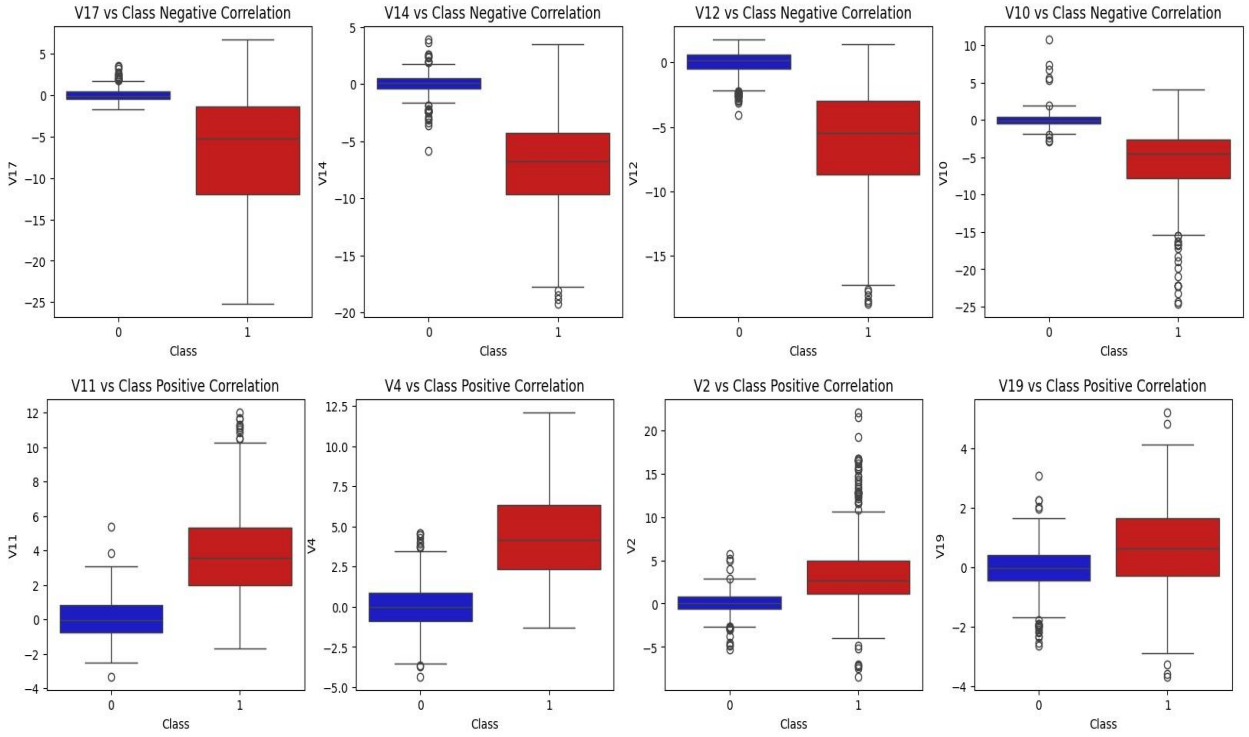

Figure 3. Box plots comparing Class 0 (non-fraud) and Class 1 (fraud) variables.

8.2. Evaluation Metrics

a) Receiver Operating Characteristic (ROC) Curve

The receiver operating characteristic (ROC) curve is a crucial tool in machine learning for assessing the precision of binary classifiers. It represents the trade-off between sensitivity and specificity at thresholds. A perfect classifier has Area Under the ROC Curve (AUC) of 1, indicating a high true-positive rate and low false-negative rate. A random classifier's ROC curve resembles the diagonal, producing an AUC of 0.5.

b) Macro Average of F1 Score (F1-macro)

The F1-score strikes the ideal balance between accuracy and recall. The trade-off between accuracy and recall is expressed in one metric. It is useful when there is an imbalance between classes, like in fraud detection, when the "Fraud" class is frequently in the minority. It calculates the F1 score for each class and then takes the average, treating all classes equally regardless of their frequency. The formula used is represented in Equation (1):

$$F1\ score_{macro} = \frac{1}{L} \sum_{i=1}^{L} \frac{2.P_i.R_i}{P_i+R_i} \quad (1)$$

where L is the number of classes, P_i is the precision, and R_i is the recall for class i.

c) Precision

Precision measures the model's accuracy in detecting fraud transactions. It is calculated as in Equation (2):

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Where, True Positives (TP) is Correctly identified fraud cases. False Positives (FP) identifies legitimate transactions incorrectly flagged as fraud. True Negatives (TN) identifies Correctly identified legitimate transactions, and False Negatives (FN) identifies Fraud cases missed by the model.

High precision means fewer false positives but may result in missing some fraud cases. For instance, if a model has a precision of 95%, it means 5% of detected fraud cases are false positives.

d) Recall

Recall indicates the model's ability to detect all actual fraud cases. It is calculated as in Equation (3):

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

A higher recall score indicates that more fraud cases are detected, but this can also lower precision if the model incorrectly flags many legitimate transactions as fraud.

In practice, finding the right balance between precision and recall is essential. For instance, a model with precision between 0.90 and 0.92 can accurately identify fraudulent transactions while still achieving a decent recall score. This balance helps in minimizing both false positives and false negatives, making logistic regression a valuable tool for effective fraud detection [9].

8.3. Compared Methods

Several techniques, including K-Nearest Neighbors (KNN), Logistic Regression and Decision Tree, were used to evaluate the Support Vector Classifier (SVC) model. The default settings utilized in the research to evaluate the model were 256 batch sizes, 0.0003 learning rates, and 256 hidden dimensions. The model's training was completed ahead of time after 100 epochs of training with the Adam optimizer. The evaluation's findings in Table 2 demonstrated the SVC model's and efficacy in identifying financial malfeasance in term of different evaluation metrics like Precision, Recall, F1-Score, Accuracy, AUC.

Table 2. Comparison between the SVC model along with other models.

Technique	Precision	Recall	F1-Score	Accuracy	AUC
KNN	0.87	0.84	0.85	0.88	0.93
Logistic Regression	0.90	0.88	0.89	0.91	0.96
Decision Tree	0.85	0.82	0.83	0.85	0.92
SVC	0.92	0.89	0.90	0.90	0.97

In terms of ROC curve evaluation, Figure 4 shows performance comparison between SVC model, and other models (KNN, Decision Tree, and Logistic Regression) in terms of true positive rates (TPR) and false positive rates (FPR). Each curve shows how well each model distinguishes between fraudulent and non-fraudulent transactions, with the AUC (Area Under the Curve).

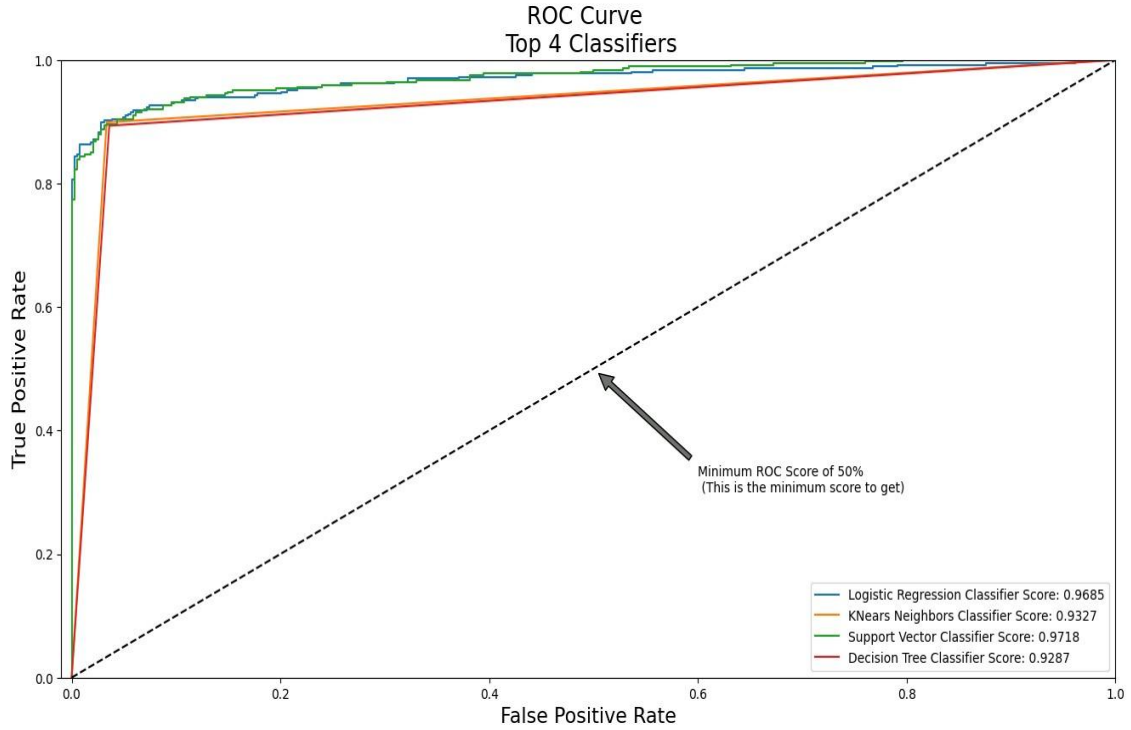

Figure 4. ROC curve evaluation.

8.4. User Interface Design

Fraud analysts can detect credit card fraud with the use of a user interface known as SPEEDD prototype. It gives a clear summary of the current level of fraud detection, allowing analysts to go further into specific cases and understand the logic behind fraud alerts. Even as technology advances, human analysts remain crucial to the fraud detection process. Common challenges include:

- Sincere purchases that, when the cardholder is not there, appear suspect.
- Varying fraud ratings obtained by computerized analysis.
- Varying institutional policies that often need human monitoring and complicated uniformity.

SPEEDD aims to overcome these gaps by providing tools to help analysts analyze and handle fraud warnings more effectively.

8.5. Fraud Detection Performance

- Used for training with a 2:1 training-to-test ratio.
- Utilizes transactions from the first 7 months as training data.
- Fraud detection is tested on transactions from August, September, and October 2021.
- This setup involves ten repetitions to ensure robustness in the results.

9. Conclusions

Credit card fraud is a serious issue in today's digital economy since credit card purchases are becoming more and more common. Enhancing the security of financial transactions requires the development of accurate and efficient fraud detection systems. This study emphasized the advantages of using data mining techniques such as decision trees and Support Vector Machines (SVMs) and looked at seven categorization methodologies for developing fraud detection models. This study found that decision tree methods, particularly C and RT regression, were more effective in identifying fraud than support vector machines (SVMs). However, SVM-based models eventually outperformed decision tree methods as training datasets increased. Financial institutions can use these algorithms to improve authorization processes and predict fraud likelihood for future transactions.

Later studies will explore additional data mining techniques, such as variations of ANNs and logistic regression, using the same real-world dataset to evaluate their effectiveness in comparison to the existing models. The SPEEDD prototype provides a method and graphical user interface for proactive event-driven decision-making, utilizing machine learning to generate new online fraud patterns and adjust to emerging forms. Analysts can make educated decisions based on automated results. Feature engineering is necessary for effective fraud pattern generation, but it may take time with large datasets. Interactive analytics techniques can improve model effectiveness. Additional metrics, like "money recall," can increase model effectiveness. Credit card fraud detection systems are crucial in e-commerce.

References

[1] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1. 2023. doi: 10.1016/j.jksuci.2022.11.008.

[2] M. Schonlau and R. Y. Zou, "The random forest algorithm for statistical learning," *Stata Journal*, vol. 20, no. 1, 2020, doi: 10.1177/1536867X20909688.

[3] Q. Li, Q. Wu, C. Zhu, J. Zhang, and W. Zhao, "An Inferable Representation Learning for Fraud Review Detection with Cold-start Problem," in *Proceedings of the International Joint Conference on Neural Networks*, 2019. doi: 10.1109/IJCNN.2019.8852437.

[4] K. Patel, "Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques," *International Journal of Computer Trends and Technology*, vol. 71, no. 10, 2023, doi: 10.14445/22312803/ijctt-v71i10p109.

[5] R. Saia and S. Carta, "Evaluating credit card transactions in the frequency domain for a proactive fraud detection approach," in *ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, 2017. doi: 10.5220/0006425803350342.

[6] R. Aitken, "U.S. Card Fraud Losses Could Exceed $12B By 2020," *Forbes*, 2016.

[7] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decis Support Syst*, vol. 50, no. 3, 2011, doi: 10.1016/j.dss.2010.08.008.

[8] L. H. Gilpin, D. Bau, B. Z. Yuan, A. Bajwa, M. Specter, and L. Kagal, "Explaining explanations: An overview of interpretability of machine learning," in *Proceedings - 2018 IEEE 5th International Conference on Data Science and Advanced Analytics, DSAA 2018*, 2018. doi: 10.1109/DSAA.2018.00018.

[9] "An Ameliorated method for Fraud Detection using Complex Generative Model: Variational Autoencoder," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 2S, pp. 262–268, Dec. 2019, doi: 10.35940/ijitee.b1005.1292s19.

[10] C. Yang, G. Liu, C. Yan, and C. Jiang, "A clustering-based flexible weighting method in AdaBoost and its application to transaction fraud detection," *Science China Information Sciences*, vol. 64, no. 12, 2021, doi: 10.1007/s11432-019-2739-2.

[11] J. W. Chang, N. Yen, and J. C. Hung, "Design of a NLP-empowered finance fraud awareness model: the anti-fraud chatbot for fraud detection and fraud classification as an instance," *J Ambient Intell Humaniz Comput*, vol. 13, no. 10, 2022, doi: 10.1007/s12652-021-03512-2.

[12] J. K. Afriyie, K. Tawiah, W. A. Pels, S. Addai-Henne, H. A. Dwamena, E. O. Owiredu, S. A. Ayeh, and J. Eshun, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, 2023, doi: 10.1016/j.dajour.2023.100163.

[13] B. Mudumba and M. F. Kabir, "Mine-first association rule mining: An integration of independent frequent patterns in distributed environments," *Decision Analytics Journal*, vol. 10, 2024, doi: 10.1016/j.dajour.2024.100434.

[14] sameh Ali and A. Raslan, "Using Data Mining Techniques for Fraud Detection in The Non-banking Sector," *Journal of Computing and Communication*, vol. 3, no. 1, 2024, doi: 10.21608/jocc.2024.339930.

[15] A. Artikis, N. Katzouris, I. Correia, C. Baber, N. Morar, I. Skarbovsky, F. Fournier, and G. Paliouras, "Industry paper: A prototype for credit card fraud management," in *DEBS 2017 - Proceedings of the 11th ACM International Conference on Distributed Event-Based Systems*, 2017. doi: 10.1145/3093742.3093912.

[16] L. AlFalahi and H. Nobanee, "Conceptual Building of Sustainable Economic Growth and Corporate Bankruptcy," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3472409.

[17] S. Xiang, M. Zhu, D. Cheng, E. Li, R. Zhao, Y. Ouyang, L. Chen, and Y. Zheng, "Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation," in *Proceedings of the 37th AAAI Conference on Artificial Intelligence, AAAI 2023*, 2023. doi: 10.1609/aaai.v37i12.26702.

[18] D. Cheng, S. Xiang, C. Shang, Y. Zhang, F. Yang, and L. Zhang, "Spatio-temporal attention-based neural network for credit card fraud detection," in *AAAI 2020 - 34th AAAI Conference on Artificial Intelligence*, 2020. doi: 10.1609/aaai.v34i01.5371.

[19] W. O. Saxton, "The discrete Fourier transform," in *Advances in Imaging and Electron Physics*, 2020. doi: 10.1016/bs.aiep.2020.04.002.

[20] K. Iizuka, "The Fast Fourier Transform (FFT)," *Springer Series in Optical Sciences*, vol. 35, 2008, doi: 10.1007/978-0-387-75724-7_7.

[21] I. Brown and C. Mues, "An experimental comparison of classification algorithms for imbalanced credit scoring data sets," *Expert Syst Appl*, vol. 39, no. 3, 2012, doi: 10.1016/j.eswa.2011.09.033.

[22] M. Chaudhry, I. Shafi, M. Mahnoor, D. L. R. Vargas, E. B. Thompson, and I. Ashraf, "A Systematic Literature Review on Identifying Patterns Using Unsupervised Clustering Algorithms: A Data Mining Perspective," *Symmetry*, vol. 15, no. 9. 2023. doi: 10.3390/sym15091679.

[23] Y. Y. Abdulla and A. I. Al-Alawi, "Advances in Machine Learning for Financial Risk Management: A Systematic Literature Review," in *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, 2024, pp. 531–535. doi: 10.1109/ICETSIS61505.2024.10459536.

[24] A. Cropper, S. Dumančić, R. Evans, and S. H. Muggleton, "Inductive logic programming at 30," *Mach Learn*, vol. 111, no. 1, 2022, doi: 10.1007/s10994-021-06089-1.

[25] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences (Switzerland)*, vol. 12, no. 19. 2022. doi: 10.3390/app12199637.

[26] J. Attenberg and F. Provost, "Inactive learning?: difficulties employing active learning in practice," *ACM SIGKDD Explorations Newsletter*, vol. 12, no. 2, 2011.

[27] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *Int J Inf Secur*, vol. 1, no. 1, 2001, doi: 10.1007/s102070100002.

[28] L. Junzhi, L. Wanqing, F. Qixiang, and L. Beidian, "Research Progress of GNSS Spoofing and Spoofing Detection Technology," in *International Conference on Communication Technology Proceedings, ICCT*, 2019. doi: 10.1109/ICCT46805.2019.8947107.