IJERST

International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com
editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025
© 2025 IJERST. All Rights Reserved

Research Paper

INTELLIGENT CLASSIFICATION OF FINANCIAL TRANSACTIONS USING REAL-TIME MACHINE LEARNING TECHNIQUES

I. VasanthaKumari, Kandoori Jaya Prasad, Amujala Poorna Abishek
Department of Computer Science and Engineering (AI&ML), Kommuri Pratap Reddy Institute of Technology, Ghatkesar, Medchal, 500088.

Received: 05-6-2025 Accepted: 03-7-2025 Published: 10-7-2025

ABSTRACT

Real-time financial fraud detection has become increasingly vital for financial institutions due to the surge in digital transactions and the growing complexity of fraudulent activities. Traditional fraud detection methods, which relied heavily on rule-based systems and manual oversight, often failed to adapt to emerging fraud tactics, leading to high false positive rates and delayed responses. Earlier approaches using statistical models and threshold-based techniques proved insufficient in identifying sophisticated, evolving fraud patterns. The integration of machine learning has transformed this landscape, enabling systems to learn from historical transaction data and accurately detect subtle signs of fraud. The push toward AI-driven solutions is driven by the demand for rapid, automated fraud detection that minimizes human error and financial losses. Traditional systems struggle with adaptability, precision, and scalability, which limits their effectiveness. In contrast, the proposed AI-based approach utilizes machine learning algorithms such as support vector machines and decision trees to analyze transaction data in real time. This enhances detection speed, improves accuracy, and delivers a scalable, robust solution to combat fraud in today's dynamic digital ecosystem.

Keywords: Real-time fraud detection, AI in finance, Transaction monitoring, Risk mitigation, Support Vector Machine (SVM).

1. INTRODUCTION

In the modern digital landscape, the exponential growth of online financial transactions has brought about significant convenience and efficiency. However, this advancement has also opened the door to a surge in fraudulent activities, particularly in banking and e-commerce systems. Fraudulent transactions can result in enormous financial losses and reputational damage to businesses and customers alike. With the availability of large volumes of transactional data and the evolution of machine learning techniques, it has become increasingly feasible to detect fraudulent patterns and prevent potential threats in real time. The project presents an intelligent fraud detection system developed using the Django web framework. It leverages supervised machine learning algorithms such as Support Vector Machine (SVM) and Random Forest Classifier to classify transaction data as fraudulent or legitimate. The system allows users to upload transaction datasets, process and train predictive models, evaluate performance using metrics like accuracy, precision, recall, and F1-score, and finally, predict the likelihood of fraud for new transactions. Additionally, the system provides insightful data visualizations and behavior flow analysis using process mining techniques to enhance user understanding and traceability of the fraud detection process.

2. LITERATURE SURVEY

Akinrinola et al. [1] delve into the ethical challenges in AI development, emphasizing the necessity for transparency, fairness, and accountability. They propose strategies to navigate these dilemmas, highlighting the importance of ethical guidelines and robust governance frameworks to ensure responsible AI deployment.

Alexopoulos et al. [2] present a comprehensive roadmap for implementing predictive maintenance technologies in production systems. They discuss the integration of IoT devices and data analytics to predict equipment failures, aiming to enhance operational efficiency and reduce downtime in industrial settings.

Amarappa and Sathyanarayana [3] offer a simplified approach to data classification using Support Vector Machines (SVM). They explain the mathematical foundations of SVM and demonstrate its effectiveness in handling complex classification tasks, making it accessible for practitioners in various fields.

Angelopoulos et al. [4] survey machine learning solutions addressing faults in the Industry 4.0 era. They identify key aspects such as real-time monitoring, anomaly detection, and predictive analytics, underscoring the role of AI in maintaining system integrity and optimizing industrial processes.

Bhatla et al. [5] provide an in-depth understanding of credit card frauds, analyzing common fraud patterns and the challenges in detection. They discuss the limitations of traditional methods and advocate for advanced analytical techniques to effectively combat fraudulent activities.

Blom and Niemann [6] explore reputational risk management during supply chain disruption recovery from a triadic logistics outsourcing perspective. They emphasize the importance of communication, trust, and collaboration among stakeholders to mitigate reputational damage and ensure business continuity.

Bonatti et al. [7] discuss rule-based policy representations and reasoning in the context of semantic web technologies. They highlight the advantages of using rule-based systems for policy enforcement, enabling more dynamic and adaptable decision-making processes in digital environments.

Chatterjee et al. [8] examine the application of digital twin technology for credit card fraud detection. They identify opportunities and challenges, suggesting that digital twins can enhance real-time monitoring and detection capabilities, thereby improving fraud prevention strategies.

Kak [9] investigates the evolution of Zero Trust security models and their impact on transforming enterprise security. The study underscores the shift from traditional perimeter-based security to a more robust, identity-centric approach, enhancing protection against sophisticated cyber threats.

Kamuangu [10] reviews the use of AI and machine learning in financial fraud detection. The study highlights various algorithms and their effectiveness in identifying fraudulent activities, advocating for the integration of AI to enhance accuracy and efficiency in fraud detection systems.

3. PROPOSED SYSTEM

The proposed system aims to detect fraudulent financial transactions using machine learning techniques, specifically Support Vector Machines (SVM). By leveraging historical transaction data, the system identifies patterns indicative of fraud, enabling real-time detection and prevention. The implementation involves several key steps

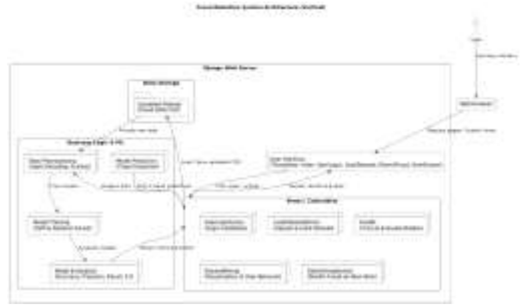


Fig. 1: Proposed Block Diagram

ML Model Building

Building the machine learning model involves selecting the appropriate algorithm, in this case, SVM, and training it on the pre-processed dataset. The model learns to identify patterns associated with fraudulent transactions by analyzing the relationships between different features. Hyperparameter tuning is performed to optimize the model's performance, and cross-validation techniques are employed to ensure its generalizability to new, unseen data.

Proposed Algorithm

Support Vector Machines (SVMs) are supervised machine learning algorithms used for classification and regression tasks. They operate by identifying the optimal hyperplane that separates data points of different classes in an N-dimensional space. This hyperplane maximizes the margin between classes, enhancing the model's ability to generalize to new data.

How SVM Works:

SVMs aim to find the hyperplane that best divides a dataset into classes. In two-dimensional space, this hyperplane is a line; in higher dimensions, it becomes a plane or hyperplane. The data points closest to this hyperplane are termed support vectors, and they are critical in defining the position and orientation of the hyperplane. By maximizing the margin—the distance between the hyperplane and the nearest data points from each class—SVMs strive to improve classification accuracy. For datasets that are not linearly separable, SVMs employ kernel functions to map data into higher-dimensional spaces where a separating hyperplane can be identified.

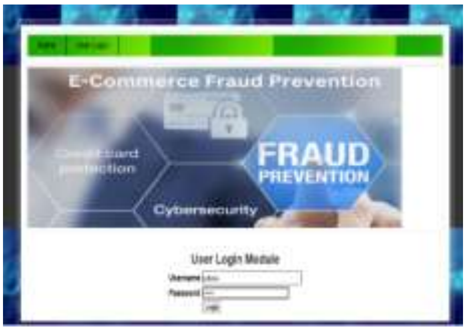
Architecture:

The architecture of a Support Vector Machine (SVM) consists of several essential components that work together to perform classification. It begins with the input layer, which receives the feature set of the data. If the data is not linearly separable, a kernel function is applied to transform the input into a higher-dimensional space where separation becomes possible. The core of the SVM is the optimization module, which solves a quadratic programming problem to find the optimal hyperplane that maximizes the margin between different classes. Finally, the output layer generates the classification result by determining on which side of the hyperplane the input data point lies.

Advantages of SVM:

SVMs perform well in scenarios where the number of features exceeds the number of samples. The use of various kernel functions allows SVMs to model complex, non-linear decision boundaries. By maximizing the margin, SVMs can reduce the risk of overfitting, especially in high-dimensional spaces. SVMs often result in models that depend only on a subset of the training data (the support vectors), making them memory efficient. SVMs can be applied to diverse data types, including text and images, making them suitable for a wide range of applications.

4. RESULTS AND DISCUSSION



User Login Module

Username

Password

Fig. 2: Login Page

The login form, accessible via the "Login" button on the homepage, presents a straightforward and secure interface for returning users. It consists of two primary input fields: "Username" and "Password." The "Username" field prompts users to enter the unique username they created during the signup process. The "Password" field, appropriately masked for security, requires users to input the corresponding password associated with their account. Below these fields, a prominent "login" button allows users to submit their credentials for verification. Upon successful authentication, users are granted access to their personalized accounts and the platform's mental health support services.

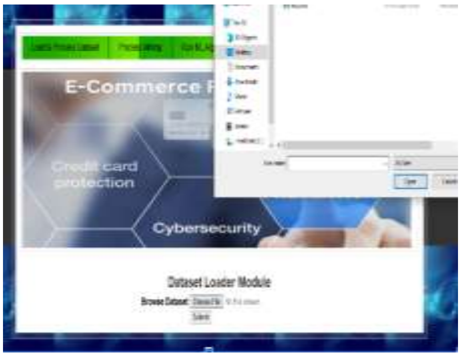


Fig. 3: Upload and processing the data

The Figure shows a portion of a web application interface for AI-based financial fraud detection. The interface of the application titled "AI-Based Financial Fraud Detection in Real-Time Transactions" is designed with a clear, workflow-oriented layout to guide users through each stage of fraud detection. At the top, a partially visible header communicates the application's main purpose. Just below, tab navigation is prominently featured with three labeled tabs: "Load & Process Dataset," "Process Mining," and "Run ML Algorithm," indicating a structured pipeline for dataset handling and machine learning execution. The "Load & Process Dataset" tab is currently active, revealing the dataset loader module. This section includes a "Browse Dataset" button that opens a file selection dialog, allowing users to locate and upload their dataset. Once a file is chosen, such as "fraud_transaction.csv" in the given example, the selected file path is displayed for confirmation. A "Submit" button is also provided to trigger the dataset loading and preprocessing stage. The interface effectively integrates user interaction elements like the overlaid file explorer titled "Select dataset," ensuring a smooth experience in navigating, uploading, and preparing data for real-time financial fraud detection.

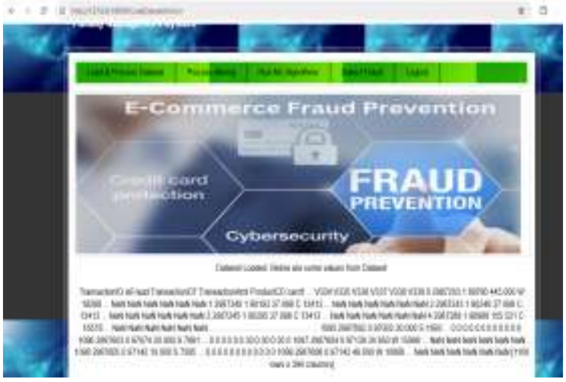
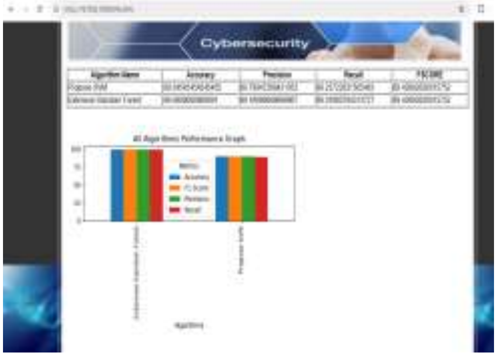


Fig. 4: Pre-processed Data

The Figure shows the data preview section of a dataset loader module in a financial fraud detection application. It confirms that a dataset has been loaded and provides a glimpse into the data's structure, including transaction IDs, fraud labels, amounts, and other anonymized features. The large number of columns suggests a rich dataset with many potential factors used for fraud detection.



Algorithm Name	Accuracy	Precision	Recall	FSCORE
Propose SVM	[illegible]	[illegible]	[illegible]	[illegible]
Extension Random Forest	[illegible]	[illegible]	[illegible]	[illegible]

Fig. 5: Comparison of

This Figure shows a comparison of the performance of two machine learning algorithms: Propose SVM and Extension Random Forest. The table presented in the interface summarizes the performance evaluation of different machine learning algorithms used for financial fraud detection, focusing on four key metrics. Each row represents an algorithm, with columns displaying the Algorithm Name, Accuracy, Precision, Recall, and FSCORE (F1-Score). These metrics provide a comprehensive view of each model's effectiveness, where Accuracy measures the overall correctness of predictions, Precision indicates the proportion of correctly identified fraud cases among all predicted frauds, Recall shows the ability to detect actual frauds, and FSCORE balances both Precision and Recall. The "Propose SVM" row lists the performance of the proposed Support Vector Machine model, achieving an accuracy of 89.54%, while the "Extension Random Forest" row reflects the results of an enhanced Random Forest model, which outperforms the SVM with a significantly higher accuracy of 99.09%. Each cell in the table contains the specific calculated value for its corresponding metric, allowing users to directly compare model performance.

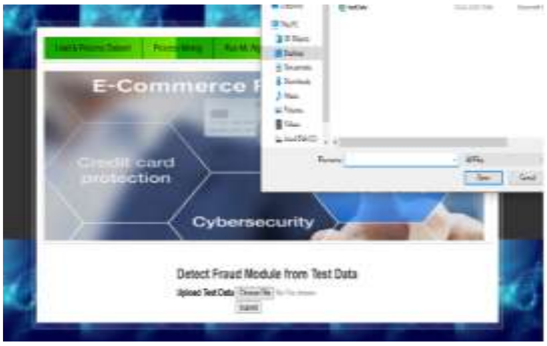


Fig. 6: upload Detect Fraud Dataset

The Figure shows the data loading phase of a financial fraud detection application. Users can select a dataset file, which will then be loaded and processed. The application will use process mining and machine learning algorithms to detect fraudulent transactions, and the "Detect Fraud Module" allows for testing the model on a separate dataset. The interface is designed to guide users through the process of data loading, model training, and evaluation.

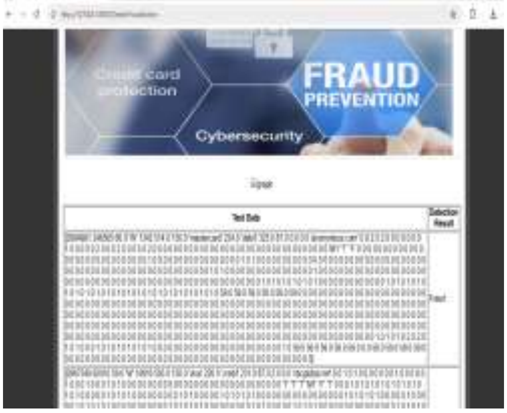


Fig. 7: Predicted Outcomes

The Figure shows the data is formatted in a way that's difficult to read directly, possibly representing anonymized or encoded transaction details. There are several rows visible, each with a long string of characters (likely representing numerical and/or categorical data). The rightmost column shows the outcome of the fraud detection process for each test case. The visible results are either Fraud or Normal.

5. CONCLUSION

The integration of Artificial Intelligence (AI) into financial fraud detection systems has significantly enhanced the ability of institutions to identify and prevent fraudulent activities. Traditional rule-based systems, while effective to a degree, often struggle to keep pace with the evolving tactics of fraudsters. AI-driven models, particularly those utilizing machine learning algorithms, offer a dynamic and adaptive approach to fraud detection. These systems can process vast amounts of transaction data in real-time, identifying complex patterns and anomalies that indicate fraudulent behavior. This capability not only improves detection rates but also reduces false positives, thereby enhancing operational efficiency and customer satisfaction. The financial sector has witnessed a substantial shift towards AI-powered solutions, with the AI in fraud detection market projected to grow at a compound annual growth rate (CAGR) of 24.5%, reaching approximately USD 108.3 billion by 2033. This growth underscores the increasing reliance on AI technologies to safeguard financial transactions. Institutions adopting these advanced systems benefit from real-time analysis, scalability, and the ability to adapt to new fraud patterns without extensive manual intervention. Moreover, AI's capacity to learn from historical data enables continuous improvement in detection capabilities, making it a formidable tool against sophisticated fraud schemes. However, the implementation of AI in fraud detection is not without challenges. Concerns regarding data privacy, the need for large datasets to train models effectively, and the potential for algorithmic biases must be addressed to ensure the ethical and effective use of AI. Additionally, the rapid advancement of AI technologies necessitates ongoing investment in infrastructure and talent to maintain and enhance system capabilities. In conclusion, AI has revolutionized financial fraud detection, offering unprecedented accuracy and efficiency in identifying fraudulent activities. As financial transactions continue to grow in volume and complexity, the role of AI in ensuring security and integrity becomes increasingly vital. By embracing AI-driven fraud detection systems, financial institutions can better protect themselves and their customers from the ever-evolving threat of fraud.

REFERENCES

[1]. Akinrinola, O., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Navigating and reviewing ethical dilemmas in AI development: Strategies for transparency, fairness, and accountability. GSC Advanced Research and Reviews, 18(3), 050-058.

[2]. Alexopoulos, K., Hribrenik, K., Surico, M., Nikolakis, N., Al-Najjar, B., Keraron, Y., Duarte, M., Zalonis, A. and Makris, S., 2021. Predictive maintenance technologies for production systems: A roadmap to development and implementation.

[3]. Amarappa, S., & Sathyanarayana, S. V. (2014). Data classification using Support vector Machine (SVM), a simplified approach. Int. J. Electron. Comput. Sci. Eng, 3, 435-445. Angelopoulos, A., Michailidis, E. T., Nomikos, N., Trakadas, P., Hatziefremidis, A.,

[4]. Voliotis, S., & Zahariadis, T. (2019). Tackling faults in the industry 4.0 era—a survey of machine-learning solutions and key aspects. Sensors, 20(1), 109.

[5]. Bhatla, T. P., Prabhu, V., & Dua, A. (2003). Understanding credit card frauds. Cards business review, 1(6), 1-15.

[6]. Blom, T., & Niemann, W. (2022). Managing reputational risk during supply chain disruption recovery: A triadic logistics outsourcing perspective.

[7]. Bonatti, P. A., De Coi, J. L., Olmedilla, D., & Sauro, L. (2009). Rule-based policy representations and reasoning. In Semantic Techniques for the Web: The REWERSE Perspective (pp. 201-232). Berlin, Heidelberg: Springer Berlin Heidelberg.

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

[9]. Kak, S. (2022). Zero Trust Evolution & Transforming Enterprise Security (Doctoral dissertation, California State University San Marcos).

[10]. Kamuangu, P. (2024). A Review on Financial Fraud Detection using AI and Machine Learning. Journal of Economics, Finance and Accounting Studies, 6(1), 67-77.