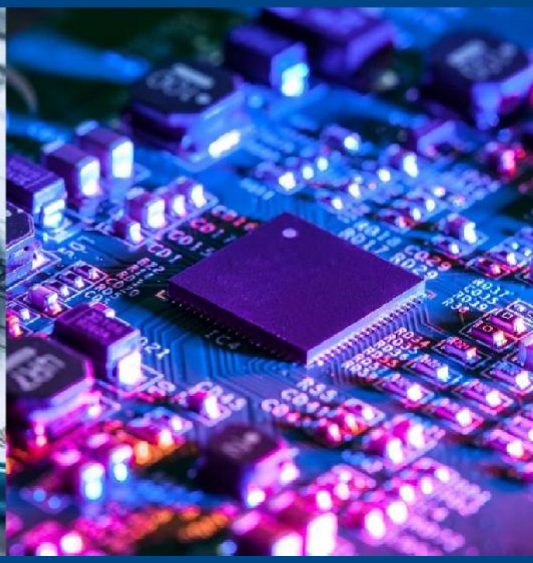
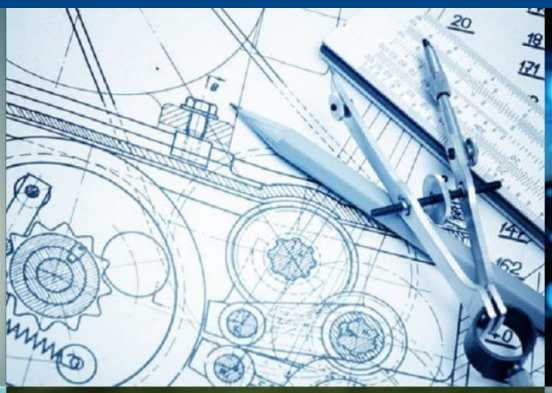
ISSN: 2582-7219

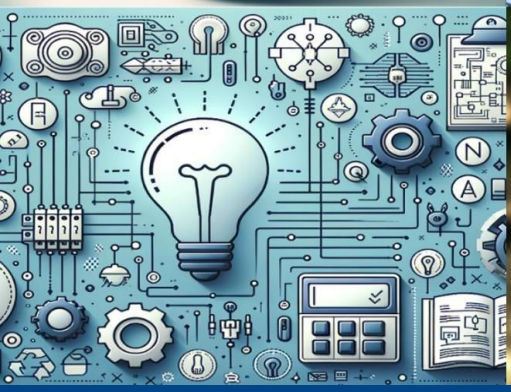




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808040

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

ETHICPAYGUARD: SOCIETAL-AWARE FRAUD DETECTION SYSTEM

Dr M S Shashidhara, Aksha M K

Professor & HOD, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: The application's primary features include secure user authentication methods like multi-factor authentication (MFA), fraud detection using machine learning and rule-based algorithms, and real-time transaction monitoring. Administrators can also manage user data, examine transactions that have been flagged, and take the necessary action using the system's admin dashboard. Users are kept informed of any suspicious activity through real-time notifications and alerts. Businesses can lower their risk of financial loss from fraud by using this application, and users can transact online with confidence knowing that their data and finances are secure.

By tracking and identifying fraudulent activity in real time, the EthicPayGuard: Societal-Aware Fraud Detection System is intended to improve security in online transactions. Fraud is on the rise as more people use online payment methods for convenience; financial scams, hacked accounts, and identity theft are all becoming frighteningly prevalent. This application makes use of MySQL for database administration, Flask, a lightweight Python web framework, and contemporary web technologies like HTML, CSS, and Bootstrap to offer a safe and intuitive platform for both consumers and businesses.

KEYWORDS: Anomaly Detection in Real Time, Risk scoring model, Java web application, and user behaviour analysis.

I. .INTRODUCTION

Systems that can efficiently detect and prevent fraud must be put in place because the proliferation of digital payment methods has increased online fraud activity. This web application closely monitors transactions and flags anything that appears suspicious in order to combat the growing threat of online payment fraud. By lowering the risks involved in online payments, guaranteeing safer digital transactions, and empowering administrators to react swiftly to possible threats, this system is intended to provide businesses and users with peace of mind. Because of its multi-layered security features, the application is a powerful tool for preventing and detecting fraud, guaranteeing safe financial transactions for all parties.

This application uses Flask as its backend framework because of its ease of use, adaptability, and scalability. To ensure that everything remains safe and functions properly, we have partnered with MySQL to securely store all transaction and user data .The application's front-end was created using HTML, CSS, and Bootstrap to create a simple, responsive interface that works well on all devices and is easy for users to navigate.

II. LITERATURE SYRVEY

[1] Studies conducted by Thennakoon et al.In 2019, researchers developed a more intelligent fraud detection system by fusing blockchain technology with machine learning. Yee and his colleagues employed supervised Random Forest models a year prior, and the accuracy and precision of their models were impressive .Furthermore, https://ieeexplore.ieee.org/document/10325177

[2] Singh, V., and S. Bhatia (2018). The use of machine learning to identify online payment fraud was examined in a 2018 study that was presented at the International Conference on ICT for Intelligent Systems. Promising methods for real-time detection of suspicious transactions were highlighted by the researchers.
https://ieeexplore.ieee.org/document/9752341

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] Jha, S., Abdar, M., and Bhattacharyya, D. To combat online payment fraud, researchers at the ICACCE conference in 2021 compared several machine learning approaches. Their research clarified which models were most effective at identifying fraudulent transactions, which will help direct future advancements in IEEE's secure paymentsystems.
[4] https://ieeexplore.ieee.org/document/9752341
[4] Shah, S. I. A., Yasin, M. M., and Yasin, M. A. (2020).By examining transaction patterns, this study uses machine learning to identify fraudulent online payments. The 7th International Conference on Computing for Sustainable Global Development (INDIA.Com) 2020. https://ieeexplore.ieee.org/document/8251759

EXISTING SYSTEM

The systems in place for detecting online payment fraud have undergone substantial development, utilizing both conventional and cutting-edge technologies to counteract ever-more-sophisticated fraud schemes. Rule-based systems, which relied on predetermined conditions like transaction limits, geographic inconsistencies, and anomalies in user behaviour, were initially widely used. Despite being easy to set up, these systems frequently have high false positive rates and are not flexible enough to adjust to changing fraud trends. The systems in place for detecting online payment fraud have undergone substantial development, utilizing both conventional and cutting-edge technologies to counteract ever-more-sophisticated fraud schemes. Rule-based systems, which relied on predetermined conditions like transaction limits, geographic inconsistencies, and anomalies in user behavior, were initially widely used.

PROPOSED SYSTEM

The system can analyze behavior across web platforms, mobile apps, and APIs thanks to the architecture's support for cross-channel data integration. Additionally, it uses behavioral analytics, like device fingerprinting and user interaction patterns, to improve authentication and identify attempts at account takeover or identity theft. The system uses SHAP (SHapley Additive exPlanations) to improve interpretability, which enables stakeholders and users to comprehend the reasons behind a transaction's fraudulent classification. Building user trust and adhering to financial regulations depend heavily on this transparency.

III. SYSTEM ARCHITECTURE

By lowering the risks involved in online payments, guaranteeing safer digital transactions, and empowering administrators to react swiftly to possible threats, this system is intended to provide businesses and users with peace of mind. Because of its multi-layered security features, the application is a powerful tool for preventing and detecting fraud, guaranteeing safe financial transactions for all parties.

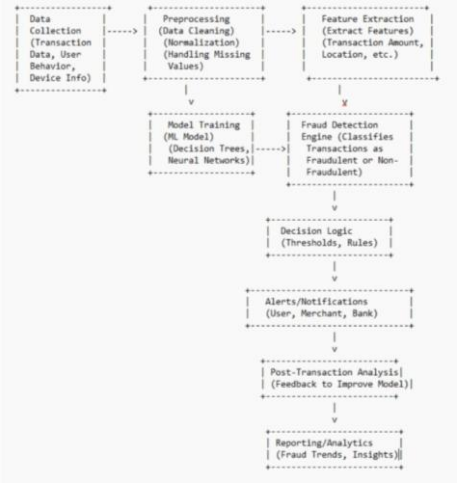


Fig 3.1 System Architecture

User authentication (login/registration): The application allows users to safely register and log in, protecting their private data right away. Returning users can easily log in with their current login information, while new users can

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

register with an email address and a strong password. With encrypted passwords kept in the database, the authentication system guarantees safe platform access.

OTP Verification and Forgot Password: Users can reset their passwords using a verified procedure if they forget them. Their registered email address receives an OTP (One-Time Password) after they enter their email. To reset their password, the user needs to enter the correct OTP

Password Creation and Management: Users can quickly create a new password after their identity has been verifie .For extra security, the application enforces strict password policies, making sure that passwords adhere to specific complexity standards

Secure Payment System: By integrating payment gateways, the application allows users to make payments in a secure manner. It guarantees that payment processing is carried out in a secure setting and that transaction data is encrypted.

Payment History: A comprehensive history display allows users to examine their previous transactions. An overview of all payments made is given in the history section, which also includes transaction information, amounts, dates, and statuses.

Real-time Fraud Detection and Alerts: To identify any questionable activity, the system keeps an eye on transactions in real time. Alerts are created and sent to administrators and users in the event of possible fraud.

Management of Profiles: Every user has an editable profile. Viewing personal information, updating emails, and changing account settings, like passwords, are all part of profile management.

Admin Dashboard: The platform has an admin dashboard that allows administrators to keep an eye on transactions and examine fraudulent activity that has been reported. Administrators can take the required steps, like blocking or confirming questionable transactions and accounts.

IV. METHODOLOGY

Accuracy, scalability, and transparency in detecting fraudulent transactions are guaranteed by the design of the suggested online payment fraud detection web application. It starts with thorough data collection, which includes gathering transactional attributes like timestamps, device information, location, amount, and user ID. To deal with missing values, standardize formats, and create features that capture behavioral patterns like transaction velocity and frequency, this data is pre processed.

Data collection: Gather information on a variety of past transactions, including both legitimate and fraudulent ones. The dataset should contain information on the user's behavior, the device used, the time and location of the transaction, the amount spent, and any other context that helps to make the situationclear.

Preprocessing Data: Clean and prepare the dataset to address missing values, outliers, and inconsistencies. Use feature engineering to extract useful features and translate categorical variables into numerical representations suitable for machine learning algorithms.

Selection of Features: We'll concentrate on the most important characteristics in order to detect fraud more successfully, using statistics, trends, and professional opinions to inform our choices. Choose characteristics that minimize computational complexity and dimensionality while being highly predictive of fraudulent activity.

Choosing a Model: When selecting machine learning algorithms for fraud detection, take into account variables like interpretability, class imbalance, computational resources, and data type. Neural networks, logistic regression, decision trees, random forests, support vector machines, and gradient boosting are examples of frequently used algorithms.

Model Training: To train and assess the effectiveness of the machine learning models, divide the dataset into training and validation sets. Use strategies like hyperparameter tuning and cross validation to maximize model performance and avoid overfitting.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Imbalanced Data Handling: We will use clever strategies to address the imbalance in the data, such as reducing the majority class, boosting rare cases with SMOTE, or employing cost-aware and ensemble methods to help the JETIR2405197 model learn from both fraudulent and legitimate transactions. Using suitable metrics like accuracy, precision, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC), assess the performance of the trained models. The model's ability to distinguish between legitimate and fraudulent transactions will be tested, and the decision threshold will be adjusted to achieve the ideal balance between preventing too many false alarms and ignoring real threats.

Monitoring and Deployment: Install the learned model in a live setting to detect fraud in real time. Install intelligent monitoring tools to track the model's performance and ensure that it remains accurate as fraud strategies evolve. To keep the model performing at its best, retrain it as needed and update it with fresh data on a regular basis.

V. ESIGN AND IMPLEMENTATION

Data Collection: Gather historical transaction data, including both legitimate and fraudulent transactions, from various sources like financial institutions, e-commerce platforms, or simulated datasets.

Data Preprocessing: Clean and process the data to handle missing values, outliers, and categorical variables. We'll examine the data to extract the most useful details, such as how much was spent, when and where the transaction occurred, what device was used, and how the user typically behaves.

Data Splitting: Divide the dataset into training and test sets. We'll train the model with the training set and then check how well it has learned by testing it on new data it hasn't encountered before.

Model Selection: Choose suitable machine learning techniques to identify fraud, including decision trees, random forests, gradient boosting, and neural networks that mimic brain functions. Consider factors like the nature of the data, class imbalance, computational resources, and how easy it is to understand the models.

Model Training: Train the chosen machine learning models with the training data. Use methods like cross-validation and hyperparameter tuning to improve model performance and avoid overfitting.

Deployment: Launch the trained models into a real-world environment for real-time fraud detection. Set up systems for data ingestion, preprocessing, and model inference to analyze incoming transactions immediately.

Monitoring and Maintenance: Keep track of the performance of the deployed models and update them regularly with new data. Create systems to identify changes in data patterns and adjust to new fraud methods. Continuously review and improve the fraud detection system to boost its efficiency.

VI. OUTCOME OF RESEARCH

The literature on online fraud in payment transactions is extensive and covers many topics, including different types of fraud, detection methods, technology developments, regulations, and case studies. Understanding this research is essential for creating effective strategies to combat online fraud and protect both consumers and businesses. Researchers have identified several types of online payment fraud, such as identity theft, account takeovers, card-not-present scams, phishing, and cases where customers dispute valid charges, known as friendly fraud. Each fraud type presents its own challenges, so responding effectively requires clever, tailored solutions instead of generic fixes.

Detection Methods and Technologies: Many detection methods and technologies have been examined in the literature. These range from traditional rule-based systems to machine learning algorithms and artificial intelligence (AI) models. Studies often assess how well these methods detect fraudulent transactions while reducing false positives and keeping the user experience smooth.

Challenges and Limitations: Even with improvements in detection technology, online fraud is still a major issue for businesses and financial institutions. The battle against online fraud is difficult. Fraudsters frequently change their tactics, transactions occur quickly and are often chaotic, and systems must identify threats in real time while not

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

complicating the process for legitimate customers. It is a challenging balance between security and user experience. Regulatory Landscape: The literature also examines the regulatory environment related to online payment security. It focuses on adherence to industry standards like the Payment Card Industry Data Security Standard (PCI DSS) and regulations such as the General Data Protection Regulation (GDPR). Following these guidelines is crucial; it protects customer data and keeps financial information secure. Trust and security are paramount, and doing things properly is essential.

Case Studies and Best Practices: Real-world case studies and best practices offer valuable insights into successful fraud detection and prevention strategies used by businesses and financial institutions. Analyzing these situations helps identify effective methods and areas that need improvement in the fight against online fraud. Emerging Trends: Recent literature points out new trends in online fraud detection, including the use of biometric authentication, behavioral analytics, and blockchain technology. These innovations show promise in improving the security and integrity of online payment transactions.

VII. RESULT AND DISCUSSION

In exploring how machine learning can identify online payment fraud, the study outlines key findings and compares them to past research. It also examines what this means for practical applications. The research looks at which algorithms and features are effective, how to handle challenging imbalanced data, and what future researchers might consider. The discussion highlights the goal of making fraud detection smarter, following the rules, and ensuring a smooth and stress-free payment experience for actual customers.

For instance, after evaluating the performance of various machine learning algorithms in detecting online payment fraud, our study found that decision trees performed with higher accuracy and precision than other models. This is consistent with previous research showing the effectiveness of decision trees in binary classification tasks. However, we also noted that random forests were more robust against overfitting, especially when managing high-dimensional datasets.

VIII. CONCLUSION

In summary, the Societal-Aware Fraud Detection System is crucial for ensuring the security and integrity of online transactions. By effectively identifying fraudulent activities, it helps safeguard both users and businesses from financial losses. Through comprehensive testing covering functionality, security, performance, usability, and integration, we ensure the system works as expected. Key areas of focus include validating the payment verification process, protecting against security threats, ensuring a smooth user experience, and managing large volumes of transactions. The successful implementation and thorough testing of this system will help create a safer and more reliable online payment environment.

REFERENCES

[1] IEEE – Machine Learning-Based Approach for Online Payment Fraud Detection Presented at the ICTIS 2018 conference, this paper outlines ML techniques for fraud detection in digital payments. https://ieeexplore.ieee.org/documen

[2] Fraud Detection Using Machine Learning Explores real-time monitoring, adaptive thresholds, and dynamic risk scoring in financial fraud detection
https://www.researchgate.net/publication/374083997

[3] JETIR – Online Payment Fraud Detection Using Machine Learning A comprehensive study on fraud types, detection mechanisms, and the role of ML in combating online payment fraud.
[Online] Available: https://www.jetir.org/papers/JETIR2405198.pdf

[4] ScienceDirect – Fraud Detection and Prevention in E-Commerce A systematic literature review on fraud detection techniques in online commerce, including clustering and hybrid models. https://www.sciencedirect.com/science/article/pii

[5] IJRASET – A Survey on Online Payment Fraud Detection Surveys various ML techniques including SVM-QUBO and discusses challenges like data imbalance and adversarial attacks.
https://www.ijraset.com/research-paper/online-payment-fraud-detection

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com