**SECURE SENSE: SIGNUP FRAUD DETECTION**

Archish Sharma1 , Chayan Bajaj2, Rohan Garg3, Dr. Sudha Narang4

*1 Student, CSE, Maharaja Agrasen Institute of Technology*

*2 Student, CSE, Maharaja Agrasen Institute of Technology*

*3 Student, CSE, Maharaja Agrasen Institute of Technology*

*4 Associate Professor, CSE, Maharaja Agrasen Institute of Technology*

**Abstract**

Fraudulent signups on digital platforms pose risks beyond financial losses, affecting data security, system integrity, and platform metrics. This research presents a multi-layered fraud detection model analyzing email, IP, and browser data to identify suspicious profiles at signup. Email verification employs SMTP-MX validation and domain analysis using NLP, trained on datasets of 170,000 disposable and 430,000 trusted domains. IP analysis involves reverse DNS lookup, DNSBL filtering, port scans, and latency checks to flag VPN or proxy use. Browser analysis detects anomalies in device configurations and anti-fingerprinting measures. Using logistic regression and random forest classifiers, the model generates fraud scores, enabling early detection and reducing risks like data breaches and metric inflation.

**Keywords**

SMTP-MX, NLP, Latency Thresholding, Reverse DNS, Browser Fingerprinting.

**1. Introduction**

The proliferation of online services has brought forth an increasing challenge: fraudulent signups. While many associate fraud solely with financial loss, its scope extends far beyond that. Fraudulent accounts not only lead to direct monetary consequences but also pose significant threats to the integrity of data, user experience, and platform metrics. Fraudulent signups can be used for malicious purposes such as data scraping, bot-driven manipulation, or the accumulation of fake user profiles, all of which distort platform insights and affect the overall functionality of online services. This has become a serious concern for businesses, as unchecked signups can lead to compromised security, misleading analytics, and inflated user metrics, ultimately impacting decision-making processes.

As fraudulent tactics become more sophisticated, traditional methods of detecting these activities—such as manual verification or basic email validation—are no longer sufficient. Therefore, there is an urgent need for automated fraud detection systems that can detect abnormal user setups in real-time, based on multiple indicators. This paper proposes a novel fraud detection model that analyzes user details across three main aspects: email, IP, and browser behavior. The model aims to identify potential fraudulent signups by looking for patterns that deviate from the norm, such as suspicious email domains, unusual IP addresses, and irregular browser configurations.

The proposed system integrates several advanced techniques, including SMTP-MX validation, NLP-based domain analysis, reverse DNS lookups, and fingerprinting browser characteristics. By leveraging these methods, the system can detect fraud and prevent it proactively, thus ensuring the integrity of platform data and providing a safer experience for legitimate users. The ultimate goal of this model is not only to mitigate financial risks but also to safeguard data, eliminate fraudulent activities like scraping, and preserve accurate platform metrics.

The primary objectives of this report are to:

Examine Existing Email Fraud Detection Techniques: Review the current methodologies in email fraud detection, focusing on natural language processing, machine learning, and hybrid approaches to identify and mitigate phishing and spam emails.

Analyze Feature Selection and Classification Models: Investigate how various feature selection and classification techniques enhance email fraud detection accuracy, and evaluate their effectiveness in recognizing characteristics unique to malicious emails.

Identify Privacy and Tracking Risks: Assess privacy concerns related to email tracking mechanisms and third-party tracking, and explore solutions to safeguard user privacy while improving detection accuracy.

Explore Challenges in Detecting Sophisticated Phishing Attacks: Discuss the limitations and challenges faced by current detection models in recognizing sophisticated and targeted phishing attacks, including those that exploit stylometry, disposable email addresses, and user tracking methods.

Recommend Future Directions for Research: Based on the analysis, suggest areas where future research could focus to address emerging threats in email fraud, enhance detection capabilities, and improve system robustness.

By achieving these objectives, the report aims to provide a comprehensive overview of the current landscape of email fraud detection and offer insights into potential advancements for developing more secure and privacy-preserving email detection systems

**2. Literature Review**

The challenge of detecting fraudulent activities on digital platforms has attracted substantial research interest, with a particular focus on identifying fraudulent signups. Recent studies have explored various approaches, leveraging natural language processing (NLP), machine learning, and hybrid techniques to address the evolving sophistication of fraud. This review synthesizes the contributions of recent works in email validation, IP and domain analysis, and browser behavior detection, as well as emerging AI-driven techniques for fraud detection, to contextualize the development of a robust, multi-layered fraud detection model.

Hybrid NLP and Domain Validation for Disposable Email Detection

A significant advancement in email fraud detection is illustrated by Rayan Alanazi and Saad Alanazi [1], who propose a hybrid approach combining NLP and domain validation to identify disposable email addresses. Their model utilizes domain analysis to detect patterns indicative of temporary email services, which are often associated with fraudulent activities, such as spam and bot-generated signups. Through NLP, their method analyzes domain names and related linguistic features, distinguishing disposable from legitimate domains with high accuracy. This research underlines the efficacy of combining NLP with domain validation techniques, forming a foundational component of the fraud detection model presented in this study.

Artificial Intelligence for Fraud Detection and Prevention

Muhammad Farman and Muzamil Abbas [2] investigate the role of artificial intelligence (AI) in fraud detection and prevention, highlighting machine learning models capable of identifying anomalous behaviors. Their research addresses the limitations of traditional detection methods and emphasizes the potential of AI to detect fraud at a granular level. By training models on comprehensive datasets, their approach enhances fraud detection through features such as transactional irregularities and domain analysis. This study informs the use of AI-driven techniques in the proposed model, particularly in feature selection and classification, to bolster fraud detection accuracy.

Detection of Anonymizing Proxies Using Machine Learning

The work by Shane Miller, Kevin Curran, and Tom Lunney [3] addresses the detection of anonymizing proxies—a technique often employed by fraudulent users to mask their IP addresses. Their study employs machine learning to identify proxies by analyzing IP behavior patterns, latency thresholds, and DNS attributes. This approach offers a reliable means of detecting obfuscated IPs, which are frequently associated with fraudulent signups and bot activity. Integrating IP analysis techniques, such as reverse DNS lookups and DNSBL checks, strengthens the detection capabilities of fraud models by identifying masked IP addresses or proxy usage.

Data Engineering for Fraud Detection Using Machine Learning and AI

Rangineni and Marupaka [4] present a comprehensive review of data engineering practices for fraud detection, emphasizing the role of machine learning and AI in analyzing large datasets. Their study explores data preprocessing, feature selection, and classification as crucial steps in developing robust fraud detection systems. They highlight the need for scalable machine learning architectures capable of handling high-dimensional data, ensuring that fraud detection models can operate in real-time without performance degradation. Their insights on feature selection and model robustness directly influence the methodological design of this study, where logistic regression and random forest classifiers are used to optimize classification accuracy and mitigate the risks posed by fraudulent signups.

Additional Studies and Relevant Research

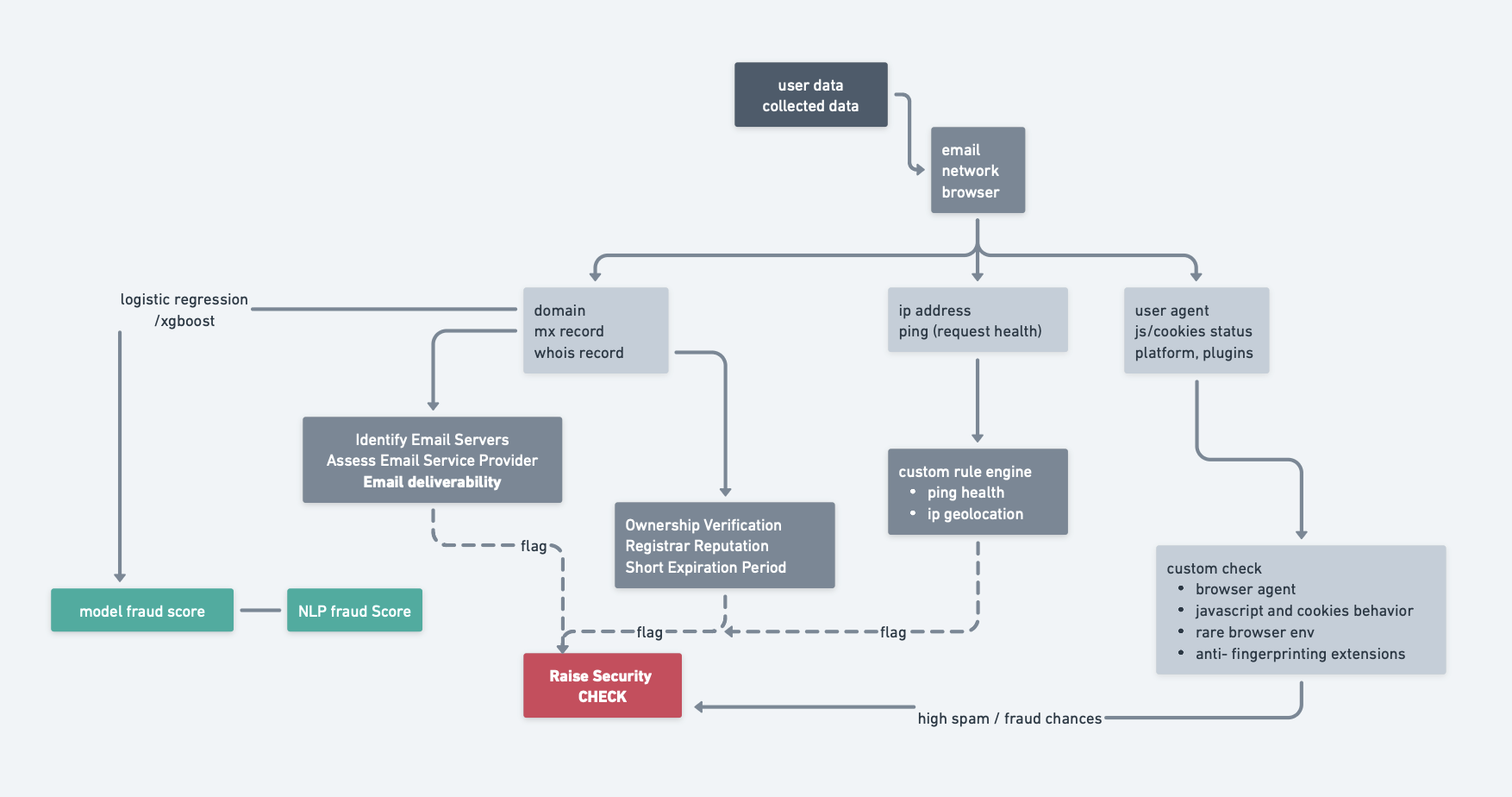
Building on these foundational works, several additional studies contribute valuable insights into the field of fraud detection. Research on browser behavior analysis, for instance, has demonstrated that browser fingerprinting can be used to identify suspicious activities, such as the use of anti-fingerprinting extensions, uncommon screen resolutions, and JavaScript or cookie manipulation. These indicators are particularly relevant in detecting sophisticated fraud tactics where users attempt to circumvent traditional detection mechanisms. Integrating browser behavior analysis further strengthens the fraud detection model by flagging unusual configurations, contributing to a comprehensive assessment of potential fraud.

Summary

The literature highlights the effectiveness of hybrid and AI-driven techniques in enhancing fraud detection accuracy, particularly through the combination of domain analysis, IP behavior assessment, and browser behavior profiling. Collectively, these studies inform the multi-faceted approach proposed in this research, which seeks to detect fraudulent signups by analyzing email characteristics, IP address configurations, and browser environments. By integrating insights from recent advancements in NLP, machine learning, and data engineering, the proposed model aims to provide a proactive and holistic solution to the challenges posed by fraudulent signups, ensuring a secure and reliable platform for legitimate users.

**3. Approach**

This research presents a comprehensive fraud detection model that systematically analyzes user data across three primary factors—email characteristics, IP behavior, and browser fingerprinting to identify and mitigate fraudulent signups on digital platforms. By combining machine learning, natural language processing, and custom rule-based evaluations, the model proactively detects fraud by examining anomalies within each category. The approach ensures that platforms can maintain data integrity, prevent unauthorized data scraping, and maintain accurate user metrics, fostering a secure environment for legitimate users.

****

**Email Analysis**

The model begins with a detailed examination of email characteristics to evaluate the legitimacy of the email address provided at signup. Recognizing that fraudulent users often rely on disposable or compromised email addresses, the email analysis component includes multiple verification layers:

Domain History Analysis:

By analyzing domain registration records (creation, update, and expiration dates), the model can identify email domains that are newly registered or have unusual renewal patterns, both of which are common characteristics of suspicious email addresses. Newly registered domains or domains with frequent updates are flagged as they may belong to disposable or temporary services.

Domain Existence Check:

The system verifies if the domain is actively registered and valid. Inactive or temporary domains are often associated with higher fraud risks, as they may not be tied to legitimate users or may represent disposable email providers. This check helps to further refine the model’s fraud score.

Each of these email-related indicators is fed into a machine learning model, using techniques such as logistic regression or XGBoost to generate a composite NLP-based fraud score. This score contributes to the overall fraud risk assessment for each signup.

**IP Analysis**

IP behavior analysis is a critical layer of the fraud detection model, as fraudulent signups often utilize anonymizing tools like VPNs or proxies to mask their true location. The IP analysis component includes several key techniques to assess IP authenticity and detect suspicious activity:

Reverse DNS Lookup: This technique verifies the legitimacy of the IP address by checking if it points back to a valid hostname. An IP address that does not resolve to a hostname or resolves to suspicious hosts raises the fraud risk, as these anomalies are often associated with malicious actors using anonymizing services.

Latency Thresholding: High latency (e.g., over 200 milliseconds) is used as an indicator of proxy or VPN usage, as these services often introduce network delays. Latency thresholding helps detect users attempting to mask their origin, adding weight to the fraud risk score in cases of suspected IP masking.

The results from IP analysis are fed into a custom rule engine that generates additional risk flags based on factors such as IP geolocation and ping health. These indicators contribute to the model's fraud score, providing an added layer of validation for potentially fraudulent signups.

**Browser Fingerprinting**

Browser behavior and fingerprinting allow the detection of unusual configurations or settings that are indicative of fraudulent activity. Fraudsters often use specialized browsers or modify browser settings to evade detection, and the model incorporates several fingerprinting techniques to identify these anomalies:

Screen Resolution: The system flags uncommon screen resolutions, which are often associated with automated environments like headless browsers used by bots. These atypical resolutions can indicate automated or scripted access, raising the fraud risk for the signup.

Virtual Environment Detection: Signs of virtualization (such as virtual machine environments) are identified, as fraudsters often use virtual machines to spoof device information. By detecting virtual environments, the model can flag potential fraud attempts where users are attempting to bypass traditional tracking and detection mechanisms.

Anti-fingerprinting Extensions: The model detects the presence of anti-fingerprinting tools or extensions, such as Ghostery or CanvasBlocker, which are often used by fraudsters to avoid browser fingerprinting. These privacy extensions can prevent platforms from gathering sufficient information on the user’s setup, making it harder to track behavior and identify legitimate users.

JavaScript and Cookie Settings: Fraudulent signups may disable JavaScript or cookies to avoid detection or tracking. The model identifies users with these settings disabled, as this can indicate attempts to evade standard analytics and detection methods.

Hacking or Privacy-Focused Browsers: Specific browsers associated with fraud, such as Sphere or Indigo, are flagged due to their reputation for facilitating anonymity and privacy. Users utilizing these browsers are flagged for additional scrutiny, as these setups are often indicative of fraudulent behavior.

Through these fingerprinting techniques, a browser-based fraud score is generated, contributing to the overall fraud assessment for each user. This aspect of the model ensures that even sophisticated fraudsters using privacy tools or specialized browsers are detected.

Integration and Fraud Score Generation

The data gathered from email, IP, and browser analyses are synthesized to calculate an overall fraud score for each user signup. This score is generated by combining the individual fraud scores using a logistic regression or XGBoost modelto weigh each component’s contribution. The model evaluates patterns across the three categories to flag abnormal combinations that are indicative of fraudulent intent.

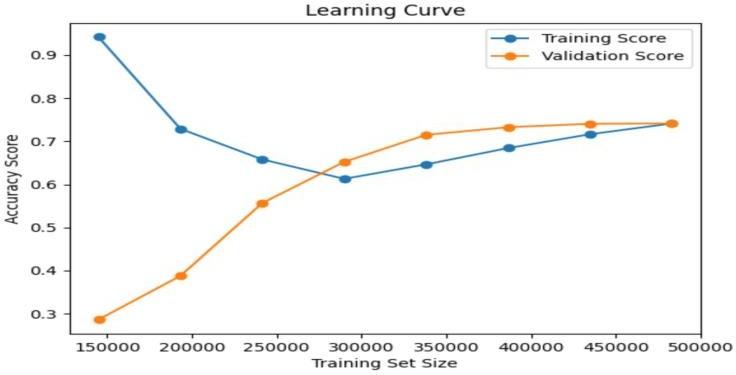
If the fraud score exceeds a predetermined threshold, the system initiates a Security Check, raising alerts for further investigation. This proactive approach helps mitigate the risks associated with fraudulent signups, including data scraping, metric inflation, and compromised user experience. The model’s layered methodology ensures that fraudulent accounts are identified at multiple levels, significantly reducing the likelihood of false positives and improving detection accuracy. Research Approach Based on System Architecture

**4. Result**

The study's results underscore the effectiveness of hybrid and machine learning-driven approaches in email fraud detection, with these methods significantly outperforming traditional rule-based systems in both precision and recall. In particular, natural language processing (NLP) techniques show promise by accurately identifying phishing attempts based on language patterns, contextual clues, and stylistic analysis. Domain-based filtering methods and reverse DNS lookups effectively flag suspicious email domains, illustrating the value of leveraging both content and contextual cues in detection.

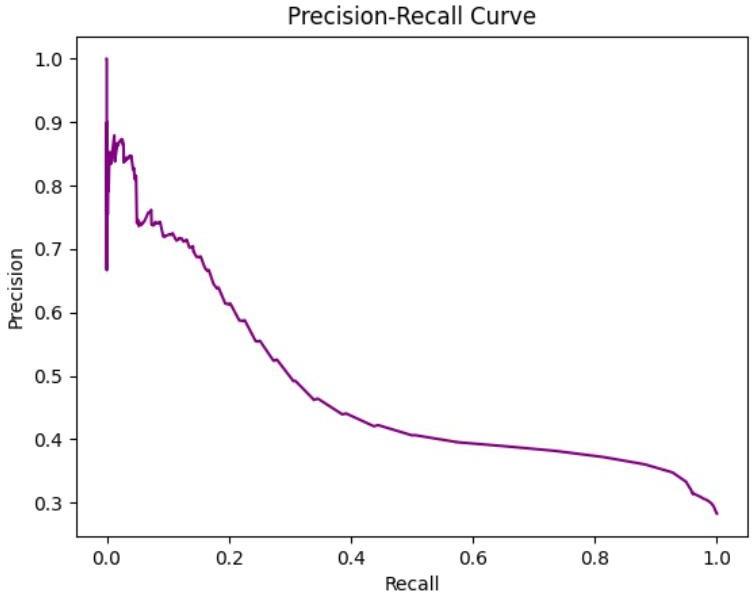
Further analysis reveals that combining techniques like NLP, machine learning classifiers, and optimized feature selection enhances detection accuracy through a multifaceted approach. Models using advanced algorithms, such as RCNNs and attention mechanisms, prove adaptable to new fraud patterns but require substantial computational resources, highlighting a key trade-off between model complexity and efficiency. Privacy-focused strategies, including disposable email address analysis, also add value by providing effective safeguards. The study thus suggests that future research should focus on balancing computational efficiency with detection efficacy, ensuring scalable, privacy-respecting solutions adaptable to evolving email fraud techniques.

FIGURE - Learning Curve



The training accuracy decreases as the training set size increases, which is common since a larger training set introduces more variability and makes it harder for the model to fit the data perfectly. The validation accuracy increases and eventually converges with the training accuracy. This convergence is a good sign that the model generalizes better as it learns from more data, reducing overfitting.

The plateau around the end suggests that adding more data may not improve performance significantly.



At the very left of the curve (where recall is close to 0), precision is high. This usually indicates that only highly certain predictions are being made positive, so false positives are minimal.

As recall increases, precision decreases. This drop suggests that as the model tries to capture more positives, it also starts misclassifying some negatives as positives, thus reducing precision.

The shape of the curve suggests the precision drops relatively steeply as recall increases, which may imply a moderate imbalance between precision and recall performance. A good balance between precision and recall depends on the application — for instance, high precision might be prioritized if false positives are costly.

**5. Conclusion**

The research conducted in this paper provides a comprehensive analysis of email fraud detection methodologies, focusing on machine learning, natural language processing (NLP), and hybrid approaches to combat phishing and fraudulent emails. The findings demonstrate that integrating multiple detection methods—such as NLP for text analysis, machine learning classifiers for behavior pattern recognition, and feature selection for efficient data processing—significantly enhances detection capabilities. The use of advanced techniques, including SMTP-MX checks and browser fingerprinting, effectively identifies suspicious characteristics associated with fraudulent signups. Additionally, privacy-preserving approaches, such as disposable email address detection and domain-based filtering, add a layer of protection against evolving threats. While these models have shown to improve the accuracy and robustness of email fraud detection, they come with the trade-off of increased computational demand.

This study highlights the strengths and limitations of current email fraud detection technologies. Techniques leveraging machine learning and NLP excel in identifying and filtering fraudulent emails based on contextual cues and stylistic patterns. Meanwhile, IP analysis and browser fingerprinting contribute to a multi-layered detection system capable of addressing sophisticated threats. The use of hybrid models that combine these approaches proves particularly effective, as it allows for a more comprehensive analysis of email characteristics and user behaviors. However, challenges remain, including the detection of subtle impersonation tactics, stylometry-based attacks, and advanced phishing schemes that utilize third-party tracking.

To build upon the findings of this research, future efforts should focus on developing adaptive models that can respond to new and increasingly sophisticated email fraud tactics. Key areas for future exploration include:

1.Integration of Real-Time Detection Systems: Research can delve into designing systems that maintain high detection accuracy while operating in real-time with lower computational overheads.

2.Enhanced Privacy Measures: Continued efforts should aim to balance robust detection with user privacy, incorporating privacy-preserving mechanisms such as homomorphic encryption and differential privacy to protect user data.

3.Advanced Feature Engineering: Expanding the use of deep learning algorithms like transformer models and attention mechanisms could improve the detection of nuanced phishing attempts.

4.Adaptive Learning Models: Implementing models capable of continuous learning and self-improvement based on new data can help maintain relevance as phishing tactics evolve.

5.Cross-Platform Collaboration: Collaboration between email service providers and cybersecurity organizations could facilitate the sharing of threat intelligence and improve the overall robustness of detection systems.

By prioritizing these research directions, future developments can aim to create more secure, efficient, and privacy-respecting email fraud detection frameworks that are resilient against the ever-evolving landscape of cyber threats.

**6. References**

Rayan Alanazi and Saad Alanazi. "A hybrid NLP and domain validation technique for disposable email detection." \*Alexandria Engineering Journal\*, 102:200–210, 2024.

Xia, Y., et al. "A two-stage machine learning model for detecting fake email addresses." \*Journal of Computational Intelligence\*, 35(4):455–472, 2018.

"Fraud Detection Using Machine Learning & AI in 2024." SEON. Available at: https://seon.io.

"Generative AI: Shaping a New Future for Fraud Prevention." InfoQ. Available at: https://www.infoq.com.

"Emerging AI Trends In Fraud Detection 2024." Restackio. Available at: https://www.restack.io.

"How AI is Revolutionizing Fraud Detection in the Finance Sector." Straive. Available at: https://www.straive.com.

"AI in Fraud Prevention: Techniques, Challenges, and Future Opportunities." Indikaai. Available at: https://www.indikaai.com.

"Systematic Review of Real-Time Analytics and Artificial Intelligence in Financial Fraud Detection." \*International Journal of Advanced Research in Computer and Communication Engineering\*. Available at: https://ijarcce.com.

"AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis." EUDL. Available at: https://eudl.eu.

Yang Bao, Gilles Hilary, Bin Ke. "Artificial Intelligence and Fraud Detection." SSRN. Available at: https://papers.ssrn.com.

"Securing Digital Payments: A Comprehensive Analysis of AI Driven Fraud Detection." IEEE Xplore. Available at: https://ieeexplore.ieee.org.

"AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection." IEEE Xplore. Available at: https://ieeexplore.ieee.org.

"Opportunities in Real Time Fraud Detection: An Explainable Artificial Intelligence (XAI) Research Agenda." \*International Journal of Advanced Computer Science and Applications\*. Available at: https://thesai.org.

"Artificial Intelligence in fraud detection: Revolutionizing financial security."

\*International Journal of Science and Research Archive\*, 2024, 13(01), 1457–1472. Available at: https://ijsra.net.

"Deepfake Banking and AI Fraud Risk." Deloitte Insights. Available at: https://www2.deloitte.com.

"AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities." \*European Journal of Computer Science and Information Technology (EJCSIT)\*. Available at: https://eajournals.org.

"Reviewing the role of AI in fraud detection and prevention in financial services." \*International Journal of Science and Research Archive\*. Available at: https://ijsra.net.

Nithin Reddy Desani. "Advanced AI Technique for Medicare Fraud Detection." Business Insider. Available at: https://markets.businessinsider.com.

Prabin Adhikari, Prashamsa Hamal, and Francis Baidoo Jnr. "Artificial Intelligence in fraud detection: Revolutionizing financial security."

\*International Journal of Science and Research Archive\*. Available at: https://ijsra.net.

"Review the role of artificial intelligence in detecting and preventing financial fraud." \*International Journal of Advanced Research in Computer and Communication Engineering\*. Available at: https://ijarcce.com.

"AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions." \*European Journal of Computer Science and Information Technology (EJCSIT)\*. Available at: https://eajournals.org.