World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Algorithms and strategies for fraud prevention on online platforms

Pratibha Sharma *

Engineering Manager, Airbnb, inc, Seattle, USA.

World Journal of Advanced Research and Reviews, 2024, 23(02), 2220–2225

Publication history: Received on 05 July 2024; revised on 20 August 2024; accepted on 23 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2462

Abstract

The topic of fraud prevention on online platforms is an urgent area in the field of information security and user protection. Modern fraud prevention algorithms and strategies include an integrated approach combining machine learning, analytical tools, and multi-layered protection systems. The key aspects are the detection of anomalies in user behavior, the use of machine learning algorithms to identify suspicious activities, as well as the integration of data verification and verification systems. Behavioral analytical models that help predict and prevent potential threats also play an important role in the fight against fraud. The effectiveness of these methods and strategies depends on their ability to adapt to evolving threats and ensure a balance between security and user convenience.

Keywords: Fraud; Fraud prevention algorithms; Online platforms; Fraud on online platforms

1. Introduction

In the context of rapid digitalization and the increasing number of online transactions, the issue of fraud prevention on online platforms is becoming increasingly relevant. Internet fraud involves the use of digital technologies to deceive and steal financial resources or confidential information. Examples include phishing, identity theft, email spoofing, and others. Effective countermeasures against such crimes require the application of modern algorithms, including the use of machine learning technologies, behavioral analytics, blockchain technologies, and multi-factor authentication. These methods enable the detection of anomalous and suspicious activities in real-time, significantly enhancing the protection of data and financial assets.

The purpose of this article is to analyze existing algorithms and strategies for preventing fraud on online platforms and to develop recommendations for their effective application.

2. Types of fraud on online platforms

Internet fraud is a crime in which perpetrators use digital technologies to steal money from users' accounts. According to statistics, losses are expected to reach $48 billion by 2023, necessitating the implementation of robust protective measures. 84% of merchants have faced attacks, highlighting the indiscriminate nature of the threat. Global losses could reach $206 billion by 2025, requiring a global fraud prevention strategy. The industry is projected to grow to $49.99 billion by 2023, intertwining technologies for protection. Demographic vulnerabilities span generations, with an average of 206,000 cyberattacks occurring per month. Global business risks exceed $343 billion, with friendly fraud predicting losses of $25 billion. Below, Figure 1 illustrates e-commerce fraud statistics for 2024. The figures are presented in billions of dollars, except for the average number of cyberattacks, which are indicated in thousands [1].

* Corresponding author: Pratibha Sharma

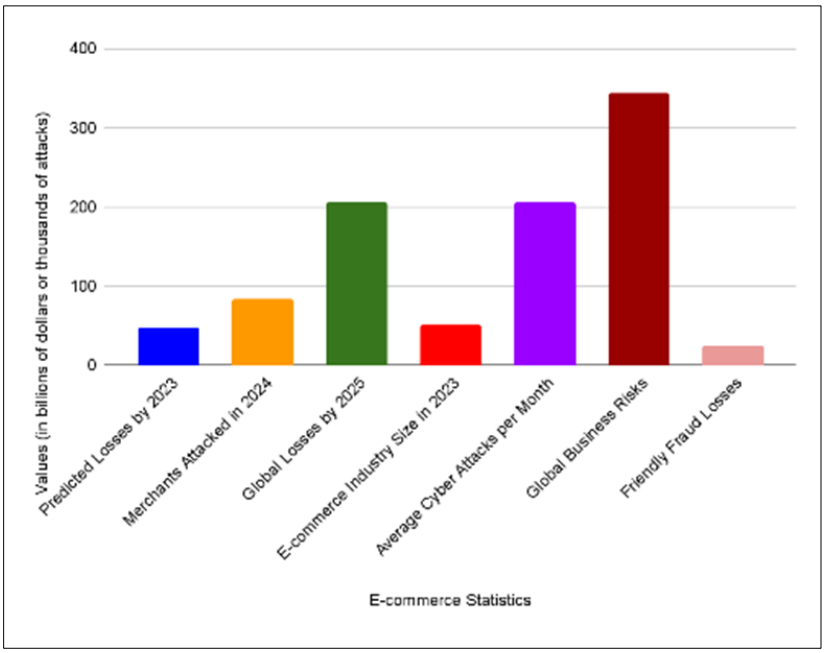

Figure 1 Statistics of fraud in e-commerce [1]

The most common types of fraud are as follows:

- Phishing: This type of fraud uses social engineering techniques to deceive users into disclosing their confidential information, such as logins, passwords, and credit card details. Attacks are often carried out via email, text messages, or fake websites that mimic legitimate resources.
- Email Spoofing: This method involves sending messages with fake sender information, creating the impression that the email comes from a trustworthy source. The goal of these attacks is to trick recipients into disclosing confidential information or launching malware.
- Overpayment Fraud: In this type of fraud, the victim is sent a check for an amount exceeding what is owed. The fraudster then asks for the difference to be returned, ultimately leading to financial losses for the victim.
- Account Takeover (ATO): ATO involves criminals gaining access to users' online accounts for financial gain. Methods include phishing, malware, and social engineering.
- SIM Swap Fraud: With the transition to LTE and 5G networks, SIM swap fraud has become more common. Criminals impersonate the owners of phone numbers and request a SIM card update, allowing them to gain access to calls, messages, and verification codes for online services.
- Identity Theft: Identity theft involves the illegal acquisition of personal information, which is then used for financial fraud or other criminal activities. This type of fraud is increasing with the rise in online shopping and banking transactions.
- Credit Card Fraud: Credit card fraud occurs when criminals deceptively obtain card details to steal money and make transactions. Sometimes enticing credit offers are used to obtain victims' data [2].

Understanding the existing types of fraudulent schemes used in e-commerce, we should now consider specific algorithms and strategies to prevent fraud.

3. Algorithms and existing strategies for fraud prevention

Detecting and preventing fraud in e-commerce is a complex task that requires a comprehensive approach. An important element is increasing security awareness and using modern technological tools to protect data. Effective measures should be based on thorough data analysis and vulnerability detection.

Compliance with PCI-DSS standards is a key aspect of ensuring security. This set of standards aims to protect the processing, storage, and transmission of credit card data. Regular PCI compliance scans help reduce the risk of vulnerabilities and protect the platform.

Another important step is SSL certification. Using SSL certificates ensures the company's authenticity and encrypts data during transmission. Payment gateways use online services to verify addresses and confirm credit card payments, enhancing overall security.

IP address analysis helps identify potential fraud. If an IP address differs from the customer's billing or shipping address or belongs to a proxy server rather than an individual account, it may indicate fraud. It is important to implement solutions to track and eliminate such discrepancies.

Multi-level authentication, such as the 3D-Secure method, offers additional protection by requiring the entry of a security code to confirm a transaction. This not only improves security but also shifts the responsibility for potential disputes from the seller to the issuing bank.

The use of complex passwords also plays a significant role in preventing fraud. Fraudsters often use programs to guess passwords, so it is important to set complex passwords and use secure platforms like Drupal 8.

To prevent chargebacks, the seller must be able to prove the authorization of the transaction by the cardholder. Otherwise, the funds are returned to the buyer, who may keep the goods. This highlights the need for careful accounting and storage of transaction information.

Customer behavior analysis using real-time analytics tools helps track visitors' movements on the site and identify suspicious actions. For example, using one credit card more than three times a week for large amounts can be restricted by certain rules.

Regular updates to shopping cart software and limiting the number of declined transactions for each account also help reduce risks. Using advanced platforms like Magento adds a level of security and helps prevent fraud.

The application of machine learning technologies, in turn, plays a crucial role in combating the most common types of fraud in e-commerce. Modern data analysis methods provide numerous tools to counter fraudulent actions. Let us consider the main mechanisms of machine learning, their functioning, and ways to apply them effectively.

Artificial Intelligence (AI) divides incoming data into normal distribution and anomalies (outliers). Anomalies represent data that deviates from standard behavior, making them suspicious. AI can analyze various types of data: images, transactions, and texts, identifying non-standard user behavior and transactions. When anomalies are detected, AI blocks or passes them on for human review. In binary tasks, such as suspicious transactions, AI can request additional confirmations from the user. However, complex decisions are better left to humans, while AI handles routine tasks, saving time [3].

The main advantage of using Machine Learning (ML) is its ability to analyze and learn from large volumes of data, making it indispensable in the face of constantly changing threats. Below, Table 1 will reflect the existing types of AI learning.

Table 1 Types of Artificial Intelligence Training[4]

Training Method	Description
Supervised Learning	These models use a labeled dataset where information is classified as legitimate or fraudulent. The main limitation is the inability to detect new types of fraud that were not present in the training data.
Unsupervised Learning	These models analyze transactions without prior labels and identify anomalies, which is useful when there is a lack of data on previous fraudulent activities.
Semi-Supervised Learning	This method is used in situations where data labeling is impossible or too costly. The model retains important parameters even if part of the data is unlabeled.
Reinforcement Learning	The model learns by interacting with the environment, adapting to various scenarios, and optimizing its actions to detect fraud.

Various industries successfully apply machine learning algorithms for fraud protection. For instance, in the e-commerce sector, companies like Airbnb and Yelp use machine learning to prevent the creation of fake accounts and account

takeovers. In the financial sector, companies such as Capgemini and Feedzai demonstrate the high efficiency of their fraud detection systems based on machine learning. These examples confirm that modern machine learning algorithms play a key role in protecting the data and financial resources of organizations [4].

Among the tools that help prevent fraud in e-commerce, the following are noteworthy:

Fraud.net is an integrated security system designed for a wide range of industries, such as finance, e-commerce, and tourism. This scalable SaaS platform uses advanced technologies, including artificial intelligence, deep learning, streaming analytics, and decision algorithms, to effectively detect and prevent fraud in real time. The system uses big data and AI to analyze and visualize information, allowing quick detection and suppression of anomalous and fraudulent transactions. It employs client account verification, internal monitoring, and custom rules, making it suitable for banking, e-commerce, and insurance. Mobile fraud is detected through device profiling and user activity tracking. The combination of real-time methods and anomaly analysis helps prevent marketing and affiliate fraud, excluding undeserved commission payments. Additionally, automated multi-factor authentication provides protection against bots and suspicious users [4].

Xceed Nice Actimize is a cloud-based solution that protects businesses from online fraud and crimes while ensuring compliance with regulatory requirements. The system's self-learning capability allows it to adapt to changing attack patterns and customer behavior, making it especially suitable for regional and credit banks. Its high-precision fraud detection system uses behavioral analytics and machine learning technologies to analyze data in real time. It provides comprehensive protection against fraud and money laundering and conducts "Know Your Customer" (KYC) and Customer Due Diligence (CDD) checks.

Kount is an AI-based tool for fraud protection in e-commerce, preventing account takeovers and bot attacks. The system reduces chargebacks and protects all stages of customer interaction. It analyzes and assesses the trust level of individuals involved in transactions, using both supervised and unsupervised machine learning to process vast amounts of data. It allows for the establishment of custom risk thresholds and prevents both new and existing fraud cases.

Adjust Fraud Prevention Suite proactively blocks a wide range of fraud, particularly advertising fraud, using automated filters that detect and reject dishonest installations and traffic [5]. The system ensures data reliability through multi-level encryption and automatic detection and blocking of suspicious traffic, such as click injections and SDK spoofing. It also highlights anomalies in click-to-install times (CTIT).

IDVision from TransUnion with iovation is a comprehensive solution for online threat protection that combines machine learning with traditional data processing methods. It automatically predicts risks and protects against various types of online fraud, such as credit card fraud and account takeovers.

RSA Adaptive Authentication uses risk assessment technologies and machine learning for accurate fraud detection. The system is suitable for both on-premises and cloud deployment, providing flexibility and scalability in protection.

AppsFlyer Protect360 protects companies from advertising fraud using machine learning algorithms that analyze client traffic throughout the user journey, detecting and preventing suspicious activities. The system uses a multi-level approach to detect and prevent fraud in real-time, ensuring payment only for genuine installs and employing behavioral biometrics to block bots [6].

Thus, reliable tools must ensure continuous monitoring of all transactions, user behavior, devices, and other indicators. They analyze this data and calculate risk scores to identify potentially fraudulent activities, such as illegal purchases, system access, advertising spam, bot actions, and the use of stolen cards. While it is impossible to completely eliminate fraud, a multi-layered approach that includes advanced security methods and tools, robust authentication, and other solutions can significantly reduce the number of illegal transactions and activities. Unfortunately, there is no universal solution to protect businesses from all types of fraud. Therefore, it is necessary to apply a multi-tiered strategy and diverse security tools tailored to the specific operations of the company. These tools must provide comprehensive coverage of all possible types of fraud targeting both businesses and customers [7].

Regarding fraud prevention strategies in e-commerce, existing strategies are reflected in Table 2.

Table 2 Fraud prevention strategies in the field of E-commerce [8]

Name	Description
Customer Identity Verification	This is the first step in fraud prevention, involving the verification of customer identities when opening an account and throughout their journey. Using multiple data sources, such as biographical, documentary, and network data, allows for real-time customer verification with minimal disruption.
Risk-Based Authentication	This method adjusts the level of verification based on the risk level of each customer or transaction. Analyzing various factors, such as device fingerprints, geolocation, IP address, transaction history, and user behavior, helps determine the risk score and apply the appropriate authentication method.
Data Protection	A legal requirement that helps prevent fraud by protecting confidential data from unauthorized access or misuse. Using encryption, anonymization, or tokenization methods ensures data security and confidentiality. Following best practices for data security, such as using strong passwords, updating software, and regularly backing up data, helps companies comply with regulations.
Customer Education	Informing customers about the risks of online fraud and prevention methods helps build trust and protect users. Education includes providing tips on recognizing and reporting fraudulent activities, such as phishing emails, fake websites, and suspicious transactions. Companies can also encourage customers to use secure passwords, enable multi-factor authentication, and regularly check their accounts.
Use of Innovative Solutions	Modern tools and technologies, leveraging artificial intelligence, machine learning, and biometrics, help stay ahead of fraudsters and enhance security.

Thus, applying these strategies and advanced methods allows companies to more effectively combat internet fraud, protecting their interests and those of their customers.

4. Conclusion

In conclusion, algorithms and strategies for fraud prevention on online platforms play a critical role in ensuring user security and maintaining trust in digital services. The development of machine learning technologies and data analytics significantly enhances the ability to detect and prevent fraudulent activities early, providing more reliable and adaptive protective measures. However, to be truly effective, these methods must continuously evolve in response to new threats and fraud trends. Integrating advanced analytical tools with multi-layered protection systems and constant monitoring of user activity are key factors in achieving an optimal level of security.

References

[1] 20 Statistics of fraud in e-commerce (2024) . [Electronic resource] Access mode: https://medium.com/@info.cybernewslive/20-ecommerce-fraud-statistics-2024-15ac230e7d50 (accessed 07/22/2024).

[2] Various types of online fraud and ways to prevent them. [Electronic resource] Access mode: https://tudiptechnologies.medium.com/different-types-of-internet-fraud-and-how-to-avoid-them-caddf23f53d5 (accessed 07/22/2024).

[3] Adi Saputra Saputra, Suharjito Suharjito Fraud detection using Machine Learning in e-commerce // International Journal of Advanced Computer Science and Application. 2019. No.9 (10). pp.332-338.

[4] Hanif Khan: Types of AI. Different types of artificial intelligence systems fossguru.com/types-of-ai-different-types-of-artificial-intelligence-systems . 2021. pp. 1-13.

[5] Fraud Detection and Prevention tools for online Businesses. [Electronic resource] Access mode: https://techflares.pages.dev/posts/fraud-detection-and-prevention-tools-for-online-business / (accessed 07/22/2024).

[6] Fraud prevention: How to detect and prevent fraud on the Internet. [Electronic resource] Access mode: https://fastercapital.com/content/Fraud-prevention--How-to-Detect-and-Prevent-Fraud-Online.html (accessed 07/22/2024).

[7] Tools for fraud detection and prevention. [Electronic resource] Access mode: https://finscoreph.medium.com/tools-for-detecting-and-preventing-fraud-71c86b7b2c07 (accessed 07/22/2024).

[8] Fraud prevention technologies and strategies to protect your business. [Electronic resource] Access mode: https://www.trulioo.com/identity-verification-use-cases/fraud-prevention/fraud#strategies-to-prevent-online-fraud (accessed 07/22/2024).