УДК 665.9

# TASKS OF ANOMALY DETECTION AND FRAUD PREVENTION IN HIGH-LOAD BOOKING SYSTEMS

***Yurchenko Vladyslav***[1], *Iryna Liutenko*[2]

[1] *PhD student of the Department of Software Engineering and Management Intelligent Technologies, NTU «KhPI», Kharkiv, Ukraine*
[2] *associate professor of the department SEMIT, Ph.D. technical of science, NTU «KhPI», Kharkiv, Ukraine*
*Vladyslav.Yurchenko@cs.khpi.edu.ua*

High-load booking systems (e.g., for airlines, hotels, and events) are a fundamental component of modern e-commerce. However, they are increasingly targeted by sophisticated bot activity and fraudulent patterns. This malicious traffic, including ticket scalping, denial of inventory, and price scraping, leads to significant financial losses, reputational damage, and an unfair user experience [1].

Despite significant progress in web security, traditional defense mechanisms such as static rate-limiting, IP blacklisting, and simple CAPTCHAs are often insufficient. Modern bots are adept at mimicking human behavior, utilizing distributed networks, and rapidly adapting to static security rules [2]. This highlights the critical need for advanced models and information technologies capable of evaluating user behavior in real-time and identifying anomalous patterns within high-velocity data streams.

The aim of this report is to propose a comprehensive model and information technology for the effective detection of bot activity and fraudulent patterns, specifically tailored to the challenges of high-load booking environments. This work focuses on developing a multi-layered evaluation framework to assess user sessions for indicators of malicious intent.

The proposed information technology is based on a four-dimensional model for user activity evaluation:

1. Level of Analysis (Data Source): (e.g., network, session, client-side)
2. Type of Task (Detection Method): (e.g., signature-based, behavioral, anomaly-based)
3. Type of Fraudulent Pattern: (e.g., scalping, inventory hoarding, scraping, fake account creation)
4. Mitigation Strategy: (e.g., block, rate-limit, present advanced challenge)

At the signature-based level, fundamental processes include checking for known malicious User-Agents, analyzing HTTP request headers, and identifying requests from known bot networks or proxy services.

At the behavioral level, key tasks include analyzing session telemetry. This involves evaluating criteria such as the speed of form completion, click-stream analysis, and mouse movement patterns. For example, non-human patterns (like instantaneous form-fills or linear mouse movements) are flagged.

At the anomaly detection level, machine learning (ML) models are applied to identify activity that deviates from established baseline profiles of legitimate user behavior. Models such as Isolation Forest or Clustering (K-Means) are used to detect suspicious coordinated activity or behavioral outliers that signature-based methods would miss [3].

The most frequently studied types of tasks include:

• Real-time Session Scoring: Assigning a dynamic risk score to each user session based on aggregated metrics.

• Behavioral Fingerprinting: Creating profiles of user interaction patterns to distinguish humans from bots.

• Fraudulent Pattern Recognition: Identifying specific attack sequences, such as "sniping" (booking at the last second) or "hoarding" (holding items in a cart without intent to purchase).

• Coordinated Attack Detection: Identifying multiple distributed clients (a botnet) acting in concert [4].

Seminal studies on e-commerce [2] and airline booking systems [4] highlight the efficacy of hybrid approaches that combine rule-based heuristics with advanced machine learning for behavioral analysis.

The proposed classification framework and model outline a robust information technology for evaluating user activity in high-load booking systems. This approach allows for the benchmarking of different detection methods and the formulation of automated, risk-based mitigation decisions.

Future efforts will prioritize the testing and validation of the model using anonymized datasets from real-world high-load systems to confirm its adequacy, reliability, and performance.

**References:**

**1.** Detection of anomalous ticket purchasing behavior for concerts based on machine learning [Електрон. ресурс]. – Режим доступу: https://www.researchgate.net/publication/379259397_Detection_of_anomalous_ticket_purchasing_behavior_for_concerts_based_on_machine_learning – Detection of anomalous ticket purchasing behavior for concerts based on machine learning.

**2.** Detecting and Characterizing Web Bot Traffic in a Large E-commerce Marketplace [Електрон. ресурс]. – Режим доступу: https://www.eecis.udel.edu/~hnw/paper/esorics18.pdf – Detecting and Characterizing Web Bot Traffic in a Large E-commerce Marketplace.

**3.** Botnet detection based on traffic behavior analysis and flow intervals [Електрон. ресурс]. – Режим доступу: https://www.researchgate.net/publication/259117704_Botnet_detection_based_on_traffic_behavior_analysis_and_flow_intervals – Botnet detection based on traffic behavior analysis and flow intervals.

**4.** A Conceptual Model for AI-Powered Anomaly Detection in Airline Booking and Transaction Systems [Електрон. ресурс]. – Режим доступу: https://www.researchgate.net/publication/393050846_A_Conceptual_Model_for_AI-Powered_Anomaly_Detection_in_Airline_Booking_and_Transaction_Systems – A Conceptual Model for AI-Powered Anomaly Detection in Airline Booking and Transaction Systems.