Volodymyr Nazarenko
PhD, Associate Professor, Computer Systems, Networks and Cybersecurity Department
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-7433-2484
volodnz@nubip.edu.ua

VIDEO GAME SECURITY IN 2025: HYBRID ANTI-CHEAT ARCHITECTURES, BEHAVIORAL ANALYTICS, AND LESSONS FOR REAL-TIME CYBER-PHYSICAL SYSTEMS

Abstract. Modern online video games are real-time, data-intensive distributed systems that must detect and deter adversaries who continuously evolve their tools and tactics. At stake are fairness, revenue, and player trust. This paper systematizes hybrid anti-cheat architectures that combine client integrity controls, server-side validation, behavioral analytics, and privacy-aware AI. We argue that video game security is a mature "living laboratory" for real-time anomaly detection under latency constraints and that its techniques transfer to adjacent domains (e.g., digital twins and industrial simulations). We first outline the problem: memory injection, protocol and telemetry manipulation, botting/scripting, identity abuse, and targeted denial-of-service attacks. We developed a reference threat model, a layered control framework, and a small benchmark of statistical and machine-learning detectors (Z-score, SVM, LSTM) over synthetic but realistic action-telemetry streams. Results show that LSTM-based detectors can achieve detection accuracy exceeding 90% with modest (<15 ms) per-event overhead in server pipelines. At the same time, server-side validation and rate-limiting remain indispensable for mitigating protocol abuse. The contribution is a concise engineering playbook that aligns computer engineering practice (design for correctness, resilience, and observability) with the operational realities of video game security at scale, as well as a set of implementation patterns that can be adapted to other real-time systems.

Keywords: anti-cheat; server-side validation; behavioral analytics; anomaly detection; LSTM; telemetry integrity; bot detection; privacy-preserving ML.

1. INTRODUCTION

Online games operate under stringent constraints: millisecond-level latency, adversaries embedded in the user's device, and massive scale. Cheaters exploit client memory, input pipelines, and protocol edge cases; coordinated botting and distributed denial tactics degrade service quality. The engineering challenge is to detect and mitigate with high precision while preserving responsiveness and player privacy.

Server-side verification of client behavior, which involves replaying or validating player actions against an authoritative simulation, has been shown to effectively detect protocol inconsistencies [1]. Deep learning over multivariate telemetry (aim deltas, movement vectors, timings) enhances the detection of subtle behavioral patterns compared to static rules [2]. Practical taxonomies of game-security controls emphasize layered designs spanning kernel integrity, networking, and analytics [3]. In parallel, studies on bright, data-driven platforms underscore middleware, telemetry, and microservice patterns relevant to large-scale security observability [4], [5]. Sustainability-minded, real-time platforms highlight the importance of trusting telemetry and clarifying model decisions under regulatory constraints [6].

The article's goal. We aim to (i) formalize a hybrid anti-cheat architecture suitable for modern games, (ii) quantify detector trade-offs (accuracy/latency/false positives), and (iii) translate these patterns into portable design practices for other low-latency, real-time systems.

2. THE THEORETICAL BACKGROUNDS

We structure controls using a layered defense: (A) Client & Platform Integrity (secure boot, anti-tamper, code signing), (B) Transport & Protocol (TLS, token rotation, replay protection), (C) Authoritative Server Simulation (state rewind/rollback, limits, cooldowns),

and (D) Behavioral Analytics (statistical outliers, supervised/unsupervised ML). We model player behavior as a multivariate time series. $\mathbf{x}_t \in \mathbb{R}^d$ With temporal dependencies captured by sequence learners, anomalies are deviations from per-player baselines and cohort distributions. Formula 1 (bitmap in manuscript per template):

$$A(\mathbf{x}_{1:T}) = \mathbb{1}\{ f_\theta(\mathbf{x}_{1:T}) > \tau \} \quad (1)$$

where f_θ is an anomaly score (e.g., Mahalanobis or LSTM output), τ It is an adaptive threshold set to bound the false-positive rate.

3. RESEARCH METHODS

We screened peer-reviewed work on server-side verification [1], ML-based cheat detection [2], and operational security frameworks for game platforms [3] alongside architectural sources on telemetry-centric platforms [4]–[6].

We compiled an attack surface that includes memory/code injection, input emulation, timing/lag manipulation, API abuse, packet spoofing, botting/scripting, account/identity abuse, and service exhaustion. For each, we mapped prevent/detect/respond controls.

We generated synthetic yet realistic action-telemetry (movement vectors, fire/cooldown timings, recoil patterns) at 60-120 Hz. We evaluated: Z-score filter (per-feature standardization and tail flags), SVM (RBF kernel over windowed features), LSTM (sequence model over 2-3 s windows). Metrics: accuracy, FPR, per-event latency (end-to-end, server-side).

4. THE RESULTS AND DISCUSSION

The three detector families benchmarked (Z-score, SVM, LSTM) reflect distinct engineering trade-offs. Z-score filters are computationally trivial and therefore attractive for edge pre-screening. Still, their univariate nature inflates false positives when players (or operators, in DT analogues) legitimately explore the extremes of the skill envelope. SVMs provide a firm middle ground: robust decision boundaries in modest feature spaces, predictable latency under batching, and interpretable support vectors for post-incident analysis. LSTMs, finally, capture temporal dependencies intrinsic to fine motor control and coordinated input bursts; this explains the best-in-class accuracy in our benchmark. Yet, the correct reading of Table 1 is not “choose LSTM and forget the rest,” but rather compose the layers: a light statistical gate to cull evident noise, an SVM (or similar) to stabilize edge cases, and an LSTM to arbitrate high-confidence outcomes on contentious sequences.

Table 1

Detector performance over action-telemetry (balanced synthetic set)

Model	Accuracy	FPR	Avg. Server Latency per Event
Z-score filter	– 0.725	– 0.141	– 2.5 ms
SVM (RBF)	– 0.893	– 0.073	– 8.1 ms
LSTM (1–2 layers)	– 0.934	– 0.059	– 12.4 ms

Sequence learners excel at recognizing micro-temporal signatures (e.g., recoil compensation rhythms), but authoritative server validation is the only reliable mechanism to enforce physics, cooldowns, and conservation rules. In practice, we deploy LSTM output as a signal to prioritize validation, rather than replacing it. This prevents adversarial drift tactics (e.g., micro-aim jitter crafted to evade the learned manifold) from silently accumulating an

advantage. The hybrid loop is detect -> validate -> enforce -> learn; the last step updates thresholds only after server facts confirm the anomaly.

Production systems live or die by their tick budget. With <15 ms per event (batched inference, CPU/GPU offload, and model quantization), ML can sit inline without perceptible user impact. Two pragmatic rules follow: (i) keep synchronous paths minimal, defer low-value features to asynchronous audits; (ii) prefer micro-models at the edge (feature extraction, Z-score culling) and macro-models in the core (LSTM arbitration), joined by compact feature tensors rather than raw streams.

Cohort-only thresholds encode “average” behavior; high-skill outliers become collateral damage. Per-entity behavioral baselines (per-player in games; per-machine or per-operator in Digital Twins) reduce false positives by 15–25% in our tests. Implementation notes: Bootstrap with conservative thresholds for the first N initial sessions; switch to adaptive bounds once variance estimates stabilize. Re-seed baselines after major patches, map changes, or equipment servicing.

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This paper consolidates a hybrid anti-cheat blueprint that integrates server-side validation with ML-based behavioral analytics under tight latency budgets. Experiments indicate that sequence models can deliver high accuracy with acceptable overhead when paired with protocol-level validation and graduated responses. Future work: (i) adversarial ML defenses for input spoofing and model poisoning, (ii) federated and privacy-preserving training at scale, (iii) standardized observability (telemetry schemas, labels) to ease cross-title and cross-studio intelligence sharing.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] D. Bethea, R. A. Cochran, and M. K. Reiter, “Server-side verification of client behavior in online games,” *ACM TISSEC*, vol. 14, no. 4, pp. 1–27, 2008.
[2] J. P. Pinto, A. Pimenta, and P. Novais, “Deep learning and multivariate time series for cheat detection in video games,” *Machine Learning*, vol. 110, no. 11, pp. 3037–3057, 2021.
[3] V. Nazarenko and M. Funderburk, “Modern video games anti-cheating security issues,” *PROCEEDINGS MATERIALS XII International scientific conference GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2024'*, pp. 51-55, 2024.

[4] V. Nazarenko and B. Ostroushko, “Smart city management system utilizing micro-services and IoT-based systems,” *Енергетика і автоматика*, no. 1, pp. 29–38, 2024.

[5] V. Nazarenko, “Main factors of economic, land, and environmental impact due to rapid technological advancements,” *Environmental Informatics Review*, vol. 9, no. 1, pp. 14–25, 2023.

[6] T. Wuest, D. Romero, M. A. Khan, and S. Mittal, “The triple bottom line of smart manufacturing technologies: An economic, environmental, and social perspective,” in *The Routledge Handbook of Smart Technologies*, Routledge, 2022.

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE

FACULTY OF INFORMATION TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

PROCEEDINGS

МАТЕРІАЛИ

XIII International scientific and practical conference

XIII Міжнародної науково-практичної конференції

GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2025

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2025

13-14 November 2025

Kyiv, NULES of Ukraine

13-14 листопада 2025 року

Київ, НУБіП України

Kyiv 2025

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XIII Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2025

13-14 листопада 2025 року

Київ, НУБіП України

Київ 2025

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 18.12.2025).

Укладач: д.т.н., доцент Шкарупило В.В.

Збірник матеріалів XIII Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2025", 13–14 листопада 2025 року, НУБіП України, Київ. – К.: НУБіП України, 2025. – 206 с.

Відповідальність за зміст публікацій несуть автори.