iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** X **Month of publication:** October 2025

DOI: https://doi.org/10.22214/ijraset.2025.74611

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue X Oct 2025- Available at www.ijraset.com

The Evolution of Anti-Cheat Systems: A Literature Review of AI-Driven and Behavioral Approaches

Rylan Mathews Thomas[1], Jose V Francis[2]
[1]*Computer Science Engineering (Cyber Security) St. Joseph's College of Engineering and Technology*
[2]*Assistant Professor, Computer Science Engineering (Cyber Security) St. Joseph's College of Engineering and Technology*

Abstract: ***With the rise in popularity of online video games, cheating has become a real problem that harms the gaming experience and damages the industry's reputation. Traditional methods for catching cheaters often lag behind in detection and punishment. These methods can also be easily bypassed by new cheating tools. In response, recent research has looked into using artificial intelligence (AI) and machine learning to create better and more proactive anti-cheat systems. This review combines findings from seven key papers that suggest different AI-based strategies to fight cheating in first-person shooter (FPS) games and other online games. The strategies discussed include analyzing player behavior and in-game performance data, using visual recognition, and employing adversarial attacks. The papers show how these new methods could lead to faster and more precise cheat detection. They also address challenges like data access, the need for transparency, and the ongoing back-and-forth with cheating tactics.***

Index Terms: ***anti-cheat, video games, artificial intelligence, machine learning, computer vision, adversarial attacks, game security***

I. INTRODUCTION

The online gaming industry has become a global multi- billion-dollar market where fair competition is vital for player satisfaction and publisher trust. Cheating, particularly in com- petitive titles such as first-person shooters (FPS), undermines this integrity. Cheaters employ advanced techniques like com- puter vision–driven aimbots and object detection tools that rival genuine player skill.

Kernel-based anti-cheat solutions (e.g., Easy Anti-Cheat, Riot's Vanguard) attempt to counter this by monitoring low- level processes. While powerful, these methods suffer from critical drawbacks:

1) Privacy Concerns: deep system access raises suspicion among players.
2) Performance Impact: kernel drivers may cause crashes and latency.
3) Security Risks: vulnerabilities in drivers could be ex- ploited.
4) Evasion: attackers design kernel-level cheats that bypass detection.

To overcome these limitations, researchers are turning to AI and data-driven approaches that detect cheats via behavioral signatures, input anomalies, and vision-based evidence. This literature review surveys seven key works (2020–2024), pre- sented chronologically, highlighting their methods, strengths, and weaknesses, culminating in comprehensive defenses that integrate multiple perspectives. A summary of these method- ologies is presented in Table I.

II. LITERATURE REVIEW

A. XAI-Driven Explainable Multi-view Game Cheating Detec- tion (2020)

This study by NetEase introduced one of the first attempts at explainable cheat detection. Instead of treating cheating as a simple yes-or-no prediction, it proposed analyzing multiple views of player data; both static player attributes (account profile, rank) and dynamic in-game behavior (action se- quences, social graphs, and screenshots). Deep learning mod- els such as LSTMs and Transformers were used alongside explainability tools like SHAP to highlight which features influenced the detection. This improved both accuracy and trust in the system for operators and developers. However, the limitation was its reliance on rich backend data, which may not always be accessible, and the high complexity of maintaining multiple models [1].

B. Improvement of Online Game Anti-Cheat System based on Deep Learning (2021)

This work focused on improving the timeliness of cheat detection by using AI to simulate human judgment of on- screen events. The proposed method was a vision-based analysis of the player's perspective, using an object detection model (YOLOv5) to identify enemies in game screenshots.

By analyzing the visual information, the system could flag behavior that would be impossible for a legitimate player, aiming to provide a faster response than traditional methods. The approach also offered privacy benefits by avoiding system- level scans. However, the primary limitation was its high computational overhead for real-time video analysis and the significant risk of false positives against highly skilled players whose actions might appear superhuman to a model [2].

C. Deep Learning and Multivariate Time Series for Cheat Detection in Video Games (2021)

This paper proposed a novel, game-agnostic cheat detection method by analyzing raw Human-Computer Interaction

TABLE I
COMPARISON OF KEY METHODOLOGIES IN MODERN ANTI-CHEAT RESEARCH

Paper (Author, Year)	Primary Method	Data Source(s)	Key Strength	Key Limitation	Reference
Tao (2020)	Explainable AI (XAI)	Multi-view logs (Portrait, Behavior, Image, Graph)	High trust and transparency; comprehensive data use	High complexity and cost; reactive nature	[1]
Zhang, Q. (2021)	Object Detection (YOLOv5)	Game Screenshots	Focus on real-time detection potential; privacy-preserving	High risk of false positives; limited implementation scope	[2]
Pinto (2021)	Time Series Analysis (CNN)	Raw HCI Data (mouse/keyboard)	Game-agnostic; targets fundamental input patterns	Limited to input-manipulating cheats (e.g., aimbots)	[3]
Xiao (2023)	Mouse Movement Analysis (CNN)	`GetAxis()` Mouse Data from Game Engine	Extremely high accuracy on a specific aimbot type	Narrow focus; generalizability to commercial games is unproven	[4]
Nhu (2023)	Adversarial Attacks	In-game rendered frames	Actively disrupts cheats; imperceptible to humans	High implementation barrier; vulnerable to adversarial training	[5]
Zhao (2023)	Hybrid Supervised/ Unsupervised CV	Game Screenshots	Industrial-grade, fair, and adaptive; handles novel cheats	Relies on screenshot integrity; manual review can be a bottleneck	[6]
Zhang (2024)	Human-Inspired ML Framework (LSTMs, Ensembles)	Post-game Replay Files	Sophisticated design mimicking expert analysis; comprehensive threat coverage	High complexity; post-game analysis is not real-time	[7]

(HCI) data. The methodology treats player inputs like key presses and mouse movements as a multivariate time series, which is then classified by a Convolutional Neural Network (CNN). By focusing on universal input patterns rather than game-specific data, the system successfully detected aimbots and triggerbots with over 98% accuracy. This created a portable solution that does not require access to internal game logs. However, its main limitation was its narrow scope, as the method is ineffective against informational cheats like ESP/wallhacks that do not directly or consistently alter input behavior [3].

D. Detection of a Novel Object-Detection-Based Cheat Tool for FPS Games Using Machine Learning (2023)

This study developed a highly specific method for detecting vision-based aimbots by analyzing mouse movements. The approach collected mouse input data using the game engine's Input.GetAxis() function, which captures movement speed and direction. In a novel step, this 1D time-series data was reshaped into a 2D matrix and treated as a grayscale image, allowing a Convolutional Neural Network (CNN) to perform classification. This resulted in extremely high detection accuracy (over 99%) for the mechanical movements produced by the cheat tool. However, the key limitation was its narrow focus on a single type of aimbot, with unproven generalizability to commercial games and more sophisticated cheats that mimic human motion [4].

E. A Comprehensive Defense Approach Targeting The Com- puter Vision Based Cheating Tools in FPS Video Games (2023)

This work introduced a novel form of proactive defense against computer vision-based cheats. Instead of detecting cheaters, it uses adversarial attacks to generate imperceptible perturbations designed to make cheats fail. The methodology combined a 'defense approach' to hide real player models from object detectors and a 'penalty approach' to create fake targets in empty spaces, actively disrupting the cheater's tools. This successfully degraded the cheating experience without impacting legitimate players. However, its primary limitation was the high implementation barrier, as the technique re- quires deep modification of the game's core rendering pipeline [5].

F. VESPA: A General System for Vision-Based Extrasensory Perception Anticheating in Online FPS Games (2023)

This paper presented VESPA, an industrial-grade system for combating ESP cheats using a hybrid visual analysis frame- work. It combines a Supervised Detection Module for known cheats with an Unsupervised Detection Module to discover novel variants from game screenshots. A key innovation was its integration into a human-in-the-loop system, where Class Activation Maps (CAM) provide visual evidence (heatmaps) to human reviewers, ensuring fairness and improving the efficiency of the final ban decision. This created a practical and adaptive solution for production environments. However, its main limitation is its reactive, post-incident nature, as the workflow of screenshot capture, analysis, and manual review identifies cheaters after a match, rather than preventing the cheating in real-time [6].

G. Identify As A Human Does: A Pathfinder of Next- Generation Anti-Cheat Framework for FPS Games (2024)

This paper proposed HAWK, a next-generation, human- inspired anti-cheat framework designed to mimic the ana- lytical process of expert reviewers. Operating server-side on post-game replay files, the system uses a complex archi- tecture with distinct subsystems: an LSTM-based model for analyzing temporal player behavior, an ensembled committee of classifiers for statistical anomalies, and a deep network to check for sense-performance consistency. This approach proved highly effective on a massive, real-world dataset, outperforming official anti-cheat systems in both speed and accuracy. However, a key limitation is its reliance on post-game analysis, making it a reactive tool that cannot stop cheating in real-time during a match [7].

III. CONCLUSION

The research reviewed here shows a clear trend in anti- cheat methods. There is a noticeable shift away from in- trusive, kernel-based techniques, which pose privacy and stability risks, toward smarter, AI-driven, interpretable, and adaptable solutions. These systems use behavioral patterns, visual data, and human-computer interaction patterns to detect cheating with greater accuracy and complexity.

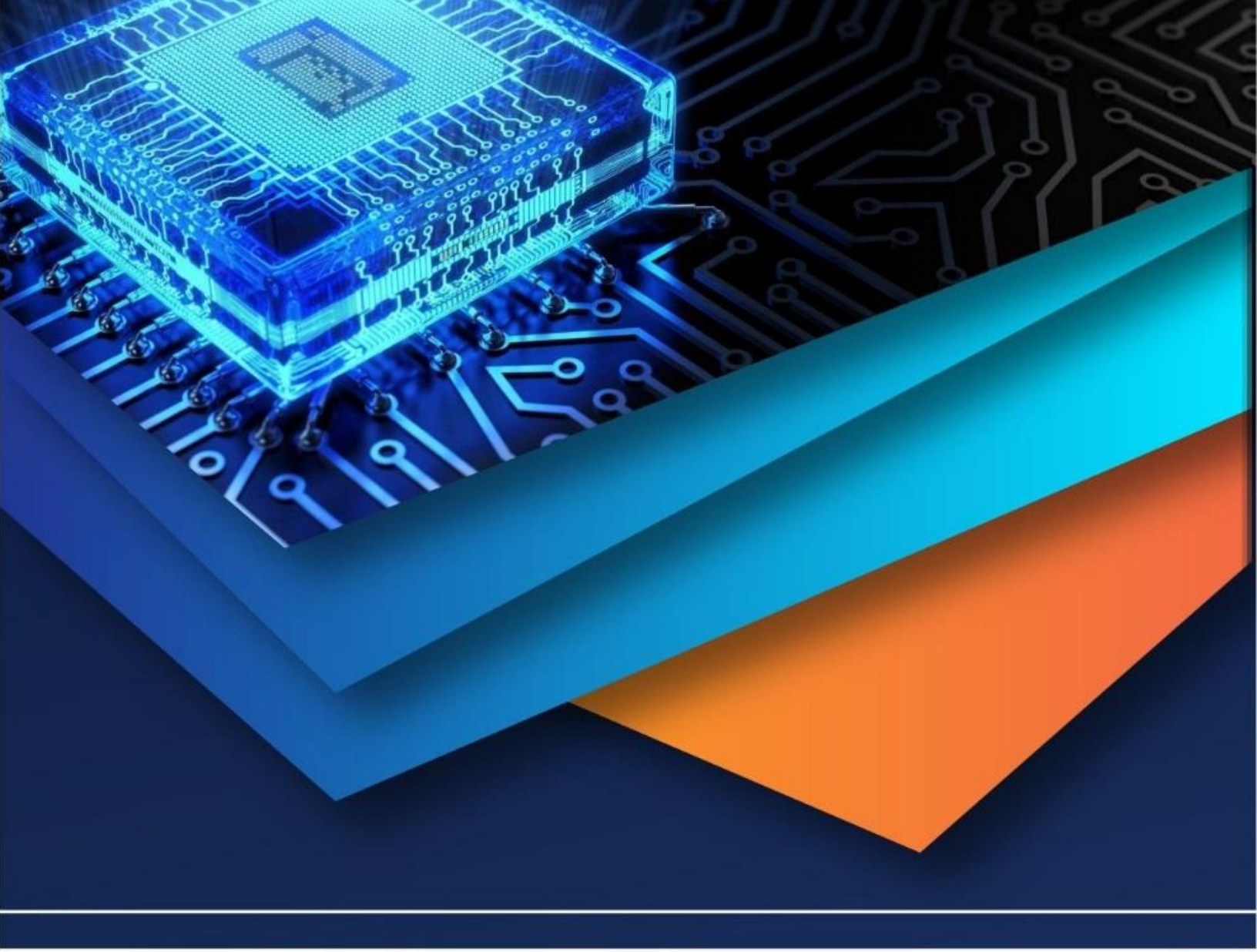
However, a key limitation remains in the literature: these approaches are mostly reactive. They are built to identify cheating only after it has happened, leading to a constant battle with cheat developers. Detection methods need frequent updates to handle new exploits. This reactive stance under- scores the need to move from just identifying bad behavior to preventing it from the start.

Our work addresses this gap by suggesting a capability architecture with memory compartmentalization. Rather than focusing on detection after the fact, this method imposes strict controls on memory access at the architectural level. This approach shifts the focus from detection to prevention, aiming to make entire categories of client-side exploits tech- nically impossible.

The future of strong game security lies in a hybrid strat- egy. This approach would use a capability architecture as a preventative base, making many common, memory- based exploits architecturally unfeasible. On top of this se- cure foundation, the adaptive AI-driven detection methods discussed in this review would act as a crucial secondary system. This system would identify new threats or hardware- based cheats that could bypass the architectural safeguards. This two-pronged strategy, which combines architectural pre- vention with behavioral detection, offers the most effective and forward-thinking path for ensuring fairness and trust in competitive gaming.

REFERENCES

[1] J. Tao, Y. Xiong, S. Zhao, Y. Xu, J. Lin, R. Wu, and C. Fan, “Xai- driven explainable multi-view game cheating detection,” in 2020 IEEE Conference on Games (CoG), pp. 144–151, 2020.
[2] Q. Zhang, “Improvement of online game anti-cheat system based on deep learning,” in 2021 2nd International Conference on Information Science and Education (ICISE-IE), pp. 652–655, 2021.
[3] J. P. Pinto, A. Pimenta, and P. Novais, “Deep learning and multivariate time series for cheat detection in video games,” in 2021 IEEE 8th Inter- national Conference on Data Science and Advanced Analytics (DSAA), pp. 1–2, 2021.
[4] Z. Xiao, T. Goto, P. Ghosh, T. Kirishima, and K. Tsuchida, “Detection of a novel object-detection-based cheat tool for first-person shooter games using machine learning,” in 2023 IEEE/ACIS 21st International Confer- ence on Software Engineering Research, Management and Applications (SERA), pp. 389–394, 2023.
[5] A. Nhu, H. Phan, C. Liu, and X. Feng, “A comprehensive defense approach targeting the computer vision based cheating tools in fps video games,” in 2023 IEEE International Performance, Computing, and Communications Conference (IPCCC), pp. 168–177, 2023.
[6] S. Zhao, J. Qi, Z. Hu, H. Yan, R. Wu, X. Shen, T. Lv, and C. Fan, “Vespa: A general system for vision-based extrasensory perception anticheating in online fps games,” IEEE Transactions on Games, vol. 16, no. 3, pp. 611– 620, 2024.
[7] J. Zhang, C. Sun, Y. Gu, Q. Zhang, J. Lin, X. Du, and C. Qian, “Identify as a human does: A pathfinder of next-generation anti-cheat framework for first-person shooter games,” arXiv preprint arXiv:2409.14830, 2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY