Critical Literature Review on Anti-Cheating Methods in FPS and Competitive Games

Group Members:
Lai Leong Chun (241UC240JR)
Teh Li Wei (1211109581)
Sow Chien Yee (1211210800)

Course: Research Methodologies for Computer Science

Assignment 1 - Critical Literature Review

Date of Submission: September 11, 2024

Abstract

Cheating in online games has become a critical issue that severely threatens fair competition and user experiences across different game platforms. Sophisticated machine learning in detecting cheating in competitive and mobile games, this work investigates some challenges such as new cheating patterns, data privacy, and limited labelled data. The four major anti-cheating frameworks reviewed here involve a deep neural network-based vision system for FPS games, few-shot learning for trajectory-based cheat detection, a bot detection system in RPG games based on behaviour evaluation and anomaly tracking, and a vision-based anti-cheat system with human supervision for large-scale industrial deployment. The most common methodologies adopted include deep neural networks, hierarchical trajectory encoding, clustering, and few-shot learning. They are pretty adaptable in new cheats and scalable across different genres. Despite the effort made so far, there are still significant gaps in cross-genre applications and real-time scalability. This work combines machine learning and human-in-the-loop systems to propose a hybrid approach that can quickly adapt to changing cheat tactics. These findings provide a foundation upon which to construct anti-cheating systems that are more secure and adaptable, with broader implications for the gaming industry as a whole.

Contents

1 Introduction

1.1 Background

Competitive gaming, often known as electronic sports or esports, is a sort of video game competition in which players compete against one another in teams or individually. In the ever-changing landscape of competitive gaming, where millions of people from across the world gather to compete in a virtual world, gameplay integrity has become an important pillar of the experience. However, as the gaming industry evolved and video games became more complicated and sophisticated, the stakes in both casual and professional gaming rose considerably. This rise has resulted in an increase in complicated cheating techniques designed to give players an unfair advantage in games. This includes aim-bots, wall-hacking, and other more advanced kinds of exploitation including DDoS attacks and network manipulation. Cheating not only undermines gaming fairness, but also damages the trust and enjoyment of honest players, leading to a toxic environment that can harm a game's player base and lifespan.

1.2 Research Problem

The issue of cheating has endured for decades, with developers and researchers always seeking to create effective anti-cheat solutions. Despite these attempts, cheating remains a chronic problem due to its increasing scope and complexity alongside the gaming industry, resulting in a never-ending cat-and-mouse chase between cheat developers and those attempting to prevent them. With the growth of esports as a real competitive arena and the increased stakes involved — both in terms of cash incentives and social status — cheating has become more profitable and, as a result, more common. Previous study has focused on a variety of facets of this topic, such as the psychological motives for cheating, the technical components of cheat design, and the efficacy of various anticheat techniques. Despite these efforts, the problem persists, and new methods of cheating emerge as fast as they are countered.

The widespread use of complex cheating tools in video games has posed significant obstacles to ensuring fair play and competitive integrity. Despite ongoing efforts to combat these cheats, existing solutions frequently fall short, resulting in a never-ending cycle of exploitation and mitigation, eventually leading to a deterioration of player experience, a loss of trust in gaming communities, and significant economic consequences for both developers and players. This ongoing problem emphasizes the need for a better knowledge of cheating methods and the development of more effective anti-cheat solutions.

1.3 Objectives and Scope

This research aims to:

1. Explore the range of current anti-cheating methods used in first-person shooter (FPS) and competitive games, and understand the effectiveness and limitations of these technologies.

2. Identify limitations or weaknesses in the existing research regarding anti-cheat methods.

3. Propose suggestions for further study or improvement to counteract cheating tactics in competitive games.

The review will focus on cheating mechanisms and anti-cheat technologies in the context of competitive gaming. A critical analysis of the viability, economy, and efficacy of current practices will be conducted. The entirety of the research reviewed will centre on the previous five (5) years because these reflect the most recent and up-to-date findings in the constantly evolving world of competitive gaming. This review will exclude casual gaming setting and focus primarily on games with significant competitive elements, where cheating poses the most severe challenges.

2 Literature Review

2.1 Overview of Selected Papers

- **Paper 1: Robust Vision-Based Cheat Detection in Competitive Gaming**
  - **Citation and Authors**: (Jonnalagadda, Frosio, Schneider, McGuire, & Kim, 2021)
  - **Research Focus**: This paper aims to improve and train the detector neutral network (DNN) in a new data set to detect visual cheats and the use of Interval Bound Propagation (IBP) to defend against adversarial attack.
  - **Methodology**:
    1. **Deep Neutral Network (DNN)**
       This is one of the data mining techniques that evaluate by creating a dataset of frames and saves the final frame buffer. The DNN will detect the visual hack in the final state that capture using Open Broadcaster Software (OBS). The OBS will capture clean and cheating images at the same time.
    2. **Interval Bound Propagation (IBP)**
       A different defence technique, IBP, a type of adversarial training to improve the reliability of DNN and fight against attacks. The IBP's position determines the upper and lower bounds of inputs and tracks the range. The final output will not be changed drastically and will remain within a safe bound.
  - **Key Findings**:
    By computing the accuracy of the DNN to detect visual hack present in the frames, there are 3 levels of cheating information (full, medium or minimum). Although most cheats were detected accurately, the system performed perfectly with medium levels of cheating information than full or minimum cheats. The use of IBP also avoids adversarial attacks to fool the DNN detector and maintains a higher accuracy of the detector.

- **Paper 2: Few-shot Learning for Trajectory-based Mobile Game Cheating Detection**
  - **Citation and Authors**: (Su et al., 2022)
  - **Research Focus**:
    This research explores a recent problem of few-shot cheating detection in mobile games, focusing on the limitations of data privacy and limited labelled data. A hierarchical framework called FCDGame was suggested to address these issues, which makes use of passively collected touch trajectories. This model generalizes characteristics from known cheating behaviours and reflects hierarchical trajectory patterns. FCDGame stands out for being secure, low in data requirements, and highly generalizable. Extensive experiments on real game datasets confirm its superior performance compared to existing cheating detection methods.
  - **Methodology**:
    Experts categorized a portion of the 800,000 touch trajectories they analysed in NetEase's mobile games, denoted as Battle and Rookie in the papers, as hacks. Through the application of DBSCAN clustering and an unsupervised seq2seq auto-encoder, they were able to discern five unique patterns of cheating that demonstrated greater regularity in comparison to typical behaviours. However, the cheating patterns change fast in mobile games. The labelled samples of novel cheating patterns are hard to obtain. So, they proposed a "Few-shot Cheating Detection method (FCDGame)" that consists of two key components: Hierarchical Trajectory Encoder and Cross-pattern Meta Learner.
    - **Hierarchical Trajectory Encoder**: Trained across multiple known cheating patterns and can be well adapted to the novel (target) cheating patterns with few labelled samples, and this encoder is also optimized with Cross-pattern Meto Learner.

    - **Cross-pattern Meta Learner**: The training consists of meta-training and fine-tuning steps. Inspired by MAML, each cheating pattern is treated as a meta task, with data split into support and query sets for training. The model's parameters are updated iteratively until convergence. In fine-tuning, new cheating patterns are used to further optimize the model, with shared encoder parameters and a classifier trained from scratch. This enables quick adaptation with minimal labelled data.

  - **Key Findings**:

    In both datasets, the suggested cheating detection approach consistently outperforms baseline techniques, especially in few-shot settings. Even with a small amount of labelled data, the Cross-pattern Meta Learner maintains excellent precision by enabling speedy adaptation to new cheating patterns. Ablation studies hightlight the usefulness of the meta-learning technique and the Hierarchical Trajectory Encoder, both of which greatly improve performance. Sensitivity analysis reveals the model's robustness and generalization capabilities in identifying a variety of cheating behaviours, even with few cheating patterns during training.

- **Paper 3: BEAT: Behavior Evaluation and Anomaly Tracking, Game Bot Detection Framework in RPG Games**

  - **Citation and Authors**: (Cao, Li, & Liang, 2024)
  - **Research Focus**: The research focuses on detecting game bots in RPGs using the BEAT (Behavior Evaluation and Anomaly Tracking) framework. It aims to:
    - Identify bots with limited labelled data (few-shot learning).
    - Analyse multiple data types (clicks, movements, game stats) to improve detection.
    - Detect repetitive patterns indicative of bot activity.
    - Create a system that adapts to new and evolving bot behaviours.
  - **Methodology**: The BEAT framework tracks cheating in RPG games by analysing different types of player trajectory data, including click, movement, game settlement, and keyboard sequences. The key methodologies involved are:
    - **Click Trajectory Sequence Model**
      - **Cycle Detection**: Identifies cyclic patterns in click trajectories using a click cycle model.
      - **Button Pattern**: Detects sub-sequences of repeated button clicks with a button cycle model.
      - **Data Transformation**: Converts sequences to seq2vec using word2vec.
      - **Model Training**: Trains CNN, RNN, RCNN, and Transformer+GAN models on the transformed data for bot detection.
    - **Moving Trajectory Sequence Model**
      - **Clustering**: Applies Kmeans, Mean Shift, and DBSCAN to cluster movement trajectory data.
      - **Cyclic Pattern Detection**: Evaluates cyclic patterns within clustered sequences to identify potential bots.
    - **Game Settlement Data Model**
      - **Data Features**: Uses settlement data (e.g., monsters killed, damage dealt) to train models such as RF, XGBoost, LightGBM, CatBoost, MLP, and Transformer.
      - **Classification**: Distinguishes between normal players and bots based on task-specific data patterns.
    - **Trajectory Image Model**
      - **Trajectory Drawing**: Converts click trajectory sequences into images, normalizing coordinates to handle varied screen resolutions.
      - **Image Classification**: Uses CNNs to classify images, exploring different models (e.g., MobileNetV3, ResNet) for optimal performance.

    - **Keyboard Trajectory Model**
        - **Pattern Analysis**: Evaluates repetition rates and periodicity in keyboard sequences to identify anomalies.
    - **Application of Bot Detection**
        - **Iterative Updates**: Regularly updates the model with new data and bot information to enhance accuracy and adaptability.
  - **Key Findings**:

    BEAT performs effectively in detecting game bots across different scenarios, including rift, instance, and field tasks. It shows high accuracy in classifying game bots due to its comprehensive approach using cyclic detection, clustering, and trajectory image models. By combining sequence analysis with machine learning models like CNN, RNN, and transformer networks, BEAT detects cheating with minimal false positives. The model adapts well to evolving cheating tactics through frequent data updates and the model.

- **Paper 4: VESPA: A General System for Vision-based Extrasensory Perception Anti-cheating in Online FPS Games**
  - **Citation and Authors**: (Zhao et al., 2023)
  - **Research Focus**: This effort presents a composition, VESPA, for anti-cheating based on vision, comprising a data preprocessing module, both supervised and unsupervised solutions. It is typically a dual-audit human-in-the-loop system for industrial gaming anti-cheating applications.
  - **Methodology**: VESPA has been developed in such a way that it captures an in-game screenshot and further processes it using In the process, labelled data would train the CNN included in the supervised learning models; hence, it would mark whether the visual features include cheating or not. An unsupervised anomaly detection module is carried out to detect novel cheats that may not have seen any training data in advance. The overall architecture of the proposed framework would be easily scalable and flexible to extend the coverage of new games with very minimal human involvement. The proposed system implements a dual audit system in which suspicious cases are reviewed by machine and human auditors.
  - **Key Findings**: The system achieves high detection rates for ESP cheats while being designed on an industrial scale. Auditing by a human in a loop can guarantee the accuracy of human reviewers, whose cheat flagging actions are verified before any penalty is applied.

2.2 Critical Analysis of Each Papers

- **Paper 1: Robust Vision-Based Cheat Detection in Competitive Gaming**
  - **Strengths**
    - **Robust Methodology**: The research paper presents a novel, vision-based approach to cheat detection, relying on DNNs to analyse the final state of the frame buffer and detect illicit overlays. This method is robust due to the use of actual in-game frames from two popular FPS games combined with three well-known cheating software tools, offering real-world relevance.
    - **Originality**: The paper's focus on vision-based detection as opposed to traditional anti-cheat methods like input monitoring is a notable innovation. This approach addresses a gap in cheat detection by leveraging machine learning to visually detect illicit overlays, a method that hadn't been thoroughly explored in prior research.
    - **Significance of Findings**: The results show that machine learning can be applied effectively to cheat detection in a practical, competitive gaming environment. The researchers' ability to differentiate between legitimate gameplay and cheating with notable accuracy could lead to more reliable and scalable anti-cheat systems in the future.
  - **Weaknesses**

    - **Sample Size and Scope**: The study is limited by the relatively small sample size of games and cheating software it analyses. Although the paper uses two popular FPS games and three cheat tools, a broader dataset encompassing a wider variety of games and cheats would provide more comprehensive results.
    - **Real-World Application**: While the vision-based method shows promise, it relies heavily on frame analysis, which may not scale well in environments with significant network latency or limited computational resources. This could affect its real-time applicability in competitive gaming scenarios where speed and efficiency are critical.
    - **Reliance on Visual Overlays**: The method primarily targets visual hacks, such as aimbots or wall-hacks, but may not be effective against more sophisticated, non-visual cheats like network manipulation or server-side exploits. This limits its utility in detecting other forms of cheating prevalent in the competitive gaming ecosystem.
  - **Relevance**

    This paper is highly relevant to our literature review as it addresses cutting-edge approaches to cheat detection, particularly in the context of FPS games. It contributes significantly to the broader understanding of anti-cheating methods by providing a new machine learning-based solution that could complement or enhance existing strategies like server-side monitoring or community reporting systems.

    The paper also offers insights into the limitations of traditional anti-cheat methods, showing how machine learning can be applied to detect cheats more efficiently and robustly. However, its narrow scope (focusing primarily on vision-based detection) could highlight a gap in our literature review, providing an opportunity to explore other methods like network monitoring or player behaviour analysis, making this paper a valuable yet specific piece in the broader anti-cheating landscape.

- **Paper 2: Few-shot Learning for Trajectory-based Mobile Game Cheating Detection**
  - **Strengths**
    - **Adaptability to Novel Cheating Patterns**: The framework's Cross-pattern Meta Learner allows it to adapt quickly to new cheating patterns, maintaining high precision even with few labelled samples.
    - **Hierarchical Trajectory Encoder**: This encoder effectively models touch trajectories, improving performance compared to other models (e.g., FCDGame outperforms its variant with a simpler encoder by up to 16% on the Rookie dataset).
    - **Generalization Capability**: The framework demonstrates strong generalization with limited cheating patterns during training, as seen in the sensitivity analysis.
    - **Robust Performance with Few Labelled Samples**: The framework performs better than baselines even in 1-shot settings, where other models struggle to detect cheating accurately.
    - **Improvement in Key Metrics**: It consistently outperforms other models in Precision, Recall, and F1-score across different datasets, especially compared to H-LSTM and MAML.
  - **Weaknesses**
    - **Performance Drop with Fewer Labelled Samples**: While FCDGame performs well, its performance still decreases as the number of labelled samples is reduced (though it remains higher than other models).
    - **Potential for Biased Learning**: The sensitivity analysis reveals that training with fewer cheating patterns can lead to biased learning, where the model focuses on specific features that may not generalize well across other patterns.
  - **Relevance**

    This article is relevant to a critical literature review on anti-cheating methods in FPS and competitive games because it addresses the challenge of detecting novel cheating patterns with minimal labelled data using the Few-shot Cheating Detection method (FCDGame). The research introduces innovative techniques such as the Hierarchical Trajectory Encoder and Cross-pattern Meta

Learner, which enhance the adaptability and precision of cheating detection frameworks. The findings on robustness with few samples and superior performance in precision, recall, and F1 score offer insight into advanced anti-cheating strategies that could be applied or adapted for FPS and competitive games, where rapid adaptation to new cheating tactics is crucial.

- **Paper 3: BEAT: Behavior Evaluation and Anomaly Tracking, Game Bot Detection Framework in RPG Games**
  - **Strengths**
    - **Automatic Updates**: Incorporates an iterative updating mechanism that improves accuracy, adapts to evolving game bots, and reduces false positives.
    - **Effectiveness**: Demonstrates successful implementation in over 30 NetEase games, saving significant amounts of revenue and receiving positive evaluations.
    - **Future Enhancements**: Plans to integrate more data types and leverage advanced algorithms (like large language models) to further improve detection capabilities and expand applicability.
  - **Weaknesses**
    - **Potential False Positives**: While the model updates to reduce false positives, there's a risk of errors, particularly if the model's predictions are incorrect before an update.
    - **Scalability and Generalization**: Although successful in RPG games, extending the model to different game types and ensuring consistent performance across diverse environments could be challenging.
  - **Relevance**

    The BEAT framework article is relevant to a critical literature review on anti-cheating methods in FPS and competitive games because it showcases advanced detection techniques for game bots in RPGs, including pattern detection, clustering, and image classification. Its methodologies and performance metrics, such as accuracy and minimal false positives, offer valuable insights into effective anti-cheating strategies that could be adapted for FPS and competitive games. Additionally, the article's discussion of strengths like automatic updates and weaknesses such as scalability issues highlights key considerations for improving anti-cheating methods across different game genres.
- **Paper 4: VESPA: A General System for Vision-based Extrasensory Perception Anti-cheating in Online FPS Games**
  - **Strengths**:
    - Combines supervised and unsupervised learning for effective detection across a wide area of cheats.
    - Designed for scalability, making it suitable for large-scale industrial applications in games.
    - Provides a dual-audit system to ensure fairness by involving human reviewers in the final decision-making process.
    - The method used in supervised learning enable the input of a set of labelled bags can reduce the cost and maintain high-quality data at the same time.
  - **Weaknesses**:
    - Acquiring unusual samples and detecting abnormal novel is costly and time consuming.
    - In supervised learning, obtaining high-quality labelled data will bring a high cost and limitation of annotation.
    - The unsupervised module may struggle with detecting novel cheating techniques, requiring continuous updates.
    - Limited focus on adversarial resistance, which could be a vulnerability in evolving cheating landscapes.

- **Relevance**:
  The VESPA system is highly relevant to the field of competitive gaming, especially in detecting ESP cheats in FPS games. Its vision-based approach effectively addresses challenges that traditional detection systems face with visual cheats. By combining supervised and unsupervised learning, VESPA can adapt to new and evolving cheats, making it ideal for large-scale deployment in the gaming industry. The human-in-the-loop auditing of the system ensures accuracy and reduces false positives, while its focus on data privacy aligns with industry standards. VESPA's adaptability across different games further enhances its relevance in the dynamic gaming environment.

2.3 Comparative Analysis and Synthesis

2.3.1 Themes and Patterns

The reviewed papers highlight a common theme of utilizing machine learning models to detect cheating in different genres of gaming. Each study emphasizes the need for adaptive, data-driven solutions to address various forms of cheating, such as visual hacks, game bots, and trajectory-based manipulations. Key methods include Deep Neural Networks (DNNs) for visual detection, few-shot learning for trajectory-based cheating, and anomaly detection for bot behaviour. Across all papers, scalability, adaptability, and accuracy are recurring concerns, especially in addressing new or evolving cheating techniques.

2.3.2 Gaps in the Literature

Several gaps remain in this body of work. First, there is limited exploration of cross-genre applications—most models are specific to a game type (e.g., FPS, mobile, RPG), leaving open the question of how well these methods generalize across different genres. Additionally, while vision-based methods and behavior analysis are well-covered, there is less focus on network-based cheating (such as server-side exploits). Another gap lies in the trade-off between real-time performance and accuracy, especially in competitive environments where latency and computational efficiency are crucial.

2.3.3 Trends

An emerging trend in cheat detection is the integration of meta-learning and few-shot learning methods to adapt to novel cheating patterns with minimal labeled data. Another trend is the use of vision-based anti-cheat systems like VESPA, which utilize a combination of supervised and unsupervised learning to detect visual cheats. Furthermore, the growing reliance on human-in-the-loop systems highlights the importance of balancing automated cheat detection with human oversight to reduce false positives and improve accuracy.

2.3.4 Synthesis

The reviewed papers collectively suggest that cheat detection is evolving toward more adaptive and scalable machine learning models that can handle a range of cheating tactics. From visual overlays in FPS games to bot detection in RPGs, the studies demonstrate that multi-modal approaches combining trajectory analysis, image recognition, and behaviour tracking are essential for effective cheat detection. However, there is still a need for more generalized frameworks that can tackle cheating across different gaming environments and integrate novel cheats without compromising real-time performance. The research thus points toward a future where machine learning models continuously evolve, incorporating frequent updates and human oversight to ensure fairness and accuracy in competitive gaming.

3 Discussions

3.1 Evaluation of the Literature

The selected body of literature provides a comprehensive view of recent developments in anti-cheating methods across various gaming platforms. The papers collectively explore a range of techniques from vision-based cheat detection, trajectory analysis, game bot detection, and novel few-shot learning approaches to combat cheating. The methodologies employed, such as Deep Neural Networks (DNNs), few-shot learning, behaviour analysis, and hierarchical encoders, contribute significantly to the field by offering more refined and adaptive anti-cheat solutions, especially as the complexity of cheating mechanisms evolves alongside competitive gaming.
However, the literature reveals a strong focus on niche areas. Articles like 'Robust Vision-Based Cheat Detection in Competitive Gaming' and 'VESPA: A General System for Vision-Based Extrasensory Perception Anti-cheating in Online FPS Games" emphasises visual hacks, while "Few-shot Learning for Trajectory-based Mobile Game Cheating Detection" and "BEAT: Behavior Evaluation and Anomaly Tracking" focus on detecting behavioural anomalies and game bot activities in mobile and RPG games. Each study approaches the problem of cheating from different angles, ranging from visual cues to player behaviour, but none offers a holistic solution to the wide range of cheating forms present in eSports, especially in FPS games.

Paper	Methodology	Key Strengths	Weaknesses
Paper 1	Vision-Based DNN	Robust frame analysis	Limited scalability
Paper 2	Few-Shot Learning	Adaptability to new cheats	Performance drops with fewer samples
Paper 3	BEAT	Effective in RPG games	Scalability issues across genres
Paper 4	VESPA	Scalable for industrial applications	Limited focus on adversarial resistance

Table 1: Comparison between Papers

Although these research papers present innovative solutions, they only partially address the overall research question, whether current anti-cheating systems are effective at keeping up with the rapidly evolving cheating tactics in competitive games. Although some approaches demonstrate adaptability to new forms of cheating, solutions tend to focus on specific aspects, such as visual hacks or movement patterns, leaving significant areas of cheating untouched. For instance, methods that target server-side exploits or network manipulation remain underexplored, which is problematic since these are common in competitive esports environments.

3.2 Gaps in Research

Several significant gaps are evident in the literature.

- **Lack of Holistic Solutions**: The reviewed literature tends to address specific types of cheating, such as visual hacks or game bots, but does not provide solutions that could tackle more diverse or complex forms of cheating, like network manipulation, server-side exploits, or more subtle social engineering cheats (e.g., exploiting game mechanics or match-fixing).

- **Limited Cross-Platform Focus**: Most papers focus on particular genres of games, such as FPS or RPGs, with minimal exploration of how anti-cheat solutions can be generalized across platforms (PC, mobile, console) or game genres. Cheating tactics may differ based on the platform, and a lack of cross-platform research leaves a significant gap.

- **Scalability and Real-Time Detection**: Papers like the "Robust Vision-Based Cheat Detection" rely on frame analysis, which poses challenges in scaling to real-time environments with high traffic and low latency requirements. More emphasis is needed on optimizing detection systems for real-time application without compromising on accuracy, especially in esports.

Games	Genre	Platform
Counter-Strike: Global Offensive	FPS	PC
Two(2) NetEase Games	FPS	Mobile
Diablo: Immortal	RPG	PC
NetEase Game	FPS	PC

Table 2: Researched Video Games in Each Paper

- **Data Privacy and Ethical Concerns**: Few papers discuss the potential privacy concerns that may arise from tracking player behaviour and collecting extensive data for cheat detection. As anti-cheat systems become more intrusive, issues around data privacy, especially in mobile and online games, need more attention. Addressing these concerns is crucial for player trust and for regulatory compliance.

3.3 Implications for Future Research

The gaps identified in the literature present several avenues for future research. These include:

- **Development of More Comprehensive Anti-Cheat Systems**: There is a clear need for solutions that can address the full spectrum of cheating methods, including both client-side and server-side exploits. Future research should explore multi-layered detection frameworks that combine visual, behavioural, and network-based data to capture a broader range of cheating tactics.

- **Cross-Platform Solutions**: Research should expand beyond specific game genres or platforms to develop anti-cheat systems that can be applied universally across PC, mobile, and console platforms. Cheating mechanisms are often platform-specific, and a generalized approach would improve scalability and flexibility.

- **Real-Time Detection and Efficiency**: As esports continues to grow, future research must focus on developing systems capable of detecting cheats in real-time, with minimal impact on performance. Solutions that incorporate lightweight machine learning models, edge computing, or more efficient data processing techniques could help achieve this.

- **Addressing Ethical and Privacy Concerns**: Research into anti-cheating methods must also consider the balance between effective cheat detection and respecting players' privacy. Future studies should explore ethical frameworks for data collection, with an emphasis on transparency, user consent, and compliance with data protection regulations.

In conclusion, while the current literature offers valuable insight into specific areas of anticheating, there remains a significant need for more holistic, cross-platform, and real-time solutions. Addressing these gaps could result in more effective and scalable anti-cheat systems, ultimately preserving the integrity of competitive gaming and improving player trust.

4 Conclusion

4.1 Summary of Key Findings

This literature review has critically examined various anti-cheat methods used in competitive gaming, particularly within FPS and RPG genres. The reviewed articles presented a diverse array of strategies for detecting cheating, ranging from visual-based detection using deep learning to few-shot learning for behavioural analysis and game bot detection. Each method demonstrates unique strengths in combating specific forms of cheating, such as visual hacks, game bots, and behavioural anomalies. However, these approaches remain fragmented, targeting isolated aspects of the broader cheating landscape without offering a holistic solution. Although advanced methodologies such as deep neural networks and hierarchical trajectory encoders have shown great promise in detecting new and evolving cheating patterns, significant limitations persist, including issues of scalability, real-time application, and generalisation across platforms and gaming genres.

4.2 Reinforce the Importance of the Research Topic

As esports continues to grow into a billion-dollar industry, the integrity of gameplay remains critical to the trust and engagement of both players and audiences. Cheating undermines the fairness and competitiveness that are the cornerstones of professional gaming, damaging not only the reputation of games and their developers but also the entire ecosystem, from casual players to professional tournaments. The stakes are high: Financial rewards, social status, and the longevity of the gaming industry all hinge on the ability to maintain a fair and secure competitive environment. This makes research into more effective anti-cheat systems an urgent priority in computer science, particularly as cheating techniques evolve rapidly alongside technological advancements.

4.3 Suggestions for Future Research

Future research should focus on developing more comprehensive, cross-platform anti-cheat systems capable of addressing a broader range of cheating methods, including server-side exploits, network manipulation, and subtle social engineering cheats. Additionally, researchers must prioritise the scalability and efficiency of these systems, ensuring that they can operate in real-time without significantly affecting gameplay performance. Integrating ethical considerations, such as data privacy and user consent, will also be critical as anti-cheat systems become more intrusive. Finally, future studies should explore the potential of multilayered detection frameworks that combine visual, behavioural, and network-based data, offering a more robust and holistic defence against the ever-evolving landscape of cheating in competitive gaming.

In conclusion, while significant progress has been made in the development of anti-cheat technologies, the challenge of maintaining fair play in esports remains an ongoing battle. By addressing the gaps identified in this review and exploring new avenues for research, the gaming industry can work toward building more effective, scalable, and ethical anti-cheat solutions that preserve the integrity of competitive gaming.

References

Cao, H., Li, Y., & Liang, Z. (2024, 02). Beat: Behavior evaluation and anomaly tracking, game bot detection framework in rpg games. *ACAI '23: Proceedings of the 2023 6th International Conference on Algorithms, Computing and Artificial Intelligence*, 309-318. Retrieved 2024-09-05, from `https://dl.acm.org/doi/10.1145/3639631.3639683` doi: 10.1145/3639631.3639683

Jonnalagadda, A., Frosio, I., Schneider, S., McGuire, M., & Kim, J. (2021, 05). Robust vision-based cheat detection in competitive gaming. *Proceedings of the ACM on Computer Graphics and Interactive Techniques*, *4*, 1-18. Retrieved 2024-09-06, from `https://dl.acm.org/doi/abs/10.1145/3451259` doi: 10.1145/3451259

Su, Y., Yao, D., Chu, X., Li, W., Bi, J., Zhao, S., ... Deng, H. (2022, 08). Few-shot learning for trajectory-based mobile game cheating detection. *Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 3941-3949. Retrieved 2024-09-09, from `https://dl.acm.org/doi/10.1145/3534678.3539157` doi: 10.1145/3534678.3539157

Zhao, S., Qi, J., Hu, Z., Yan, H., Wu, R., Shen, X., ... Fan, C. (2023, 01). Vespa: A general system for vision-based extrasensory perception anti-cheating in online fps games. *IEEE Transactions on Games*, *14*, 1-10. doi: 10.1109/tg.2023.3327115

Appendix A Member Contributions

Member	**Student ID**	**Percentage**	**Contribution**
Lai Leong Chun	241UC240JR	34%	LaTeX & BiBTeX Editor, Writer (Introduction, Discussions, Conclusion)
Teh Li Wei	1211109581	33%	Literature Researcher, Writer (Literature Review)
Sow Chien Yee	1211210800	33%	Literature Researcher, Writer (Abstract, Literature Review)

Table 3: Member Contribution