The usage of various AI models and techniques for cheat detection in online multiplayer games

Gémesi Szabolcs, Görcsös Gergely, Nagy Richárd, Szlotta Levente

2024

Abstract

If you like to spend your free time playing video games there is a high likelihood that you experienced one of the biggest problems in the gaming industry: cheating. Cheating ruins the competitive integrity of video games, and when it is widespread it can even damage the game by making the players leave the game, causing a dwindling player base. Game developers have tried numerous ways of fighting cheats, with varying success rates. A more innovative and less explored way of anti-cheat development involves artificial intelligence. This paper aims to further explore the possibility and effectiveness of using AI for cheat detection.

The problem covers a wide variety of different platforms and different types of video-games available on the market. In order to get the best results possible we try solving the problem with a combination of different AI powered techniques, namely DNNs, explainable AI and more.

By implementing, testing, and deploying our AI-driven anti-cheat solution we aim to demonstrate that AI can be more effective in identifying cheaters than traditional anti-cheating measures. Our finished system gives game developers a chance to significantly reduce cheating in their games, and maintain the integrity of competitive gaming.

1 Introduction

After so many years and so many games, online games are still so popular that the end is nowhere in sight. Millions buy not just the latest software and games but also the environment, such as PCs and consoles just to play their favorite games at their best. For them, the most terrifying thing is when they encounter cheaters in the game. Of course it is bad if you lose in the game or cannot complete the mission, but the game itself can be destroyed if there are a lot of hackers and cheaters. This work shows how game developers can prevent cheaters from appearing in the game and thereby save their product.

Filtering out the cheaters is not new. There is a lot of work, research which processes this problem and try to show how the developers can defend against it. The exact definition of our problem is that the gaming industry can't keep up with modern cheaters, and cheat developers, therefore there are several ways to cheat in recently popular games, no matter how strong the applied anti-cheat method is. In our paper, we will go through the best current methods available for game developers and using that information we will try to provide a new solution for filtering out the cheating users. We also show what the biggest drawbacks of the aforementioned researches are, why our solution is able to fill these holes and at the same time we prove why our innovation can do more than the others.

Our solution uses AI technologies such as Convolutional Neural Networks, Cross-validation, Deep Neural Networks, Explainable AI, K-Nearest Neighbour. With our innovation we are making profiles and generate scores for the user actions, with the mentioned AI technologies, and filtering out the potentially engaged users in cheating activity. We also try to cover as many online game type as possible with our system. We are trying to provide a detector app that knows after a very short time if there is a cheater in the game.

With this research we are hoping to help the game developers to develop safer games and to provide more stable games for those, who are love games, who are like to play online games. We presented this work to show that cheaters are still a problem to the gaming community, and to show that there are ways to prevent their negative impact on the gaming industry. We are hoping that with this work, we can help to reduce the cheating users in game, and also we hope that more and more new game developers and their new games will appear, because they can develop fast and effectively cheat detection to their system, which saves their product from the cheaters.

The structure of the paper is as follows: section 2 contains the most important papers of the topic with a short overview about their work. Section 4 provides our theory for cheat detection and a few examples why it works and why it is better than the current methods. Section 6 concludes the results of our research. Section 7 depicts possible further future work.

2 Related Work

2.1 Cheating and Detection Method in Massively Multiplayer Online Role-Playing Game: Systematic Literature Review [5]

The main topic of this review is the examination of possible cheat in MMORPG games, the exploration of its causes, introduction of its types and presentation of a possible detection method. In the reaserch, they discussed the structures of MMORPG games and described the types of cheating behaviours.

The authors show countermeasures to prevent cheating which comes from the structure of server and from the player's behavior. They classified the detecting methods into five groups: statistics analysis, data mining, similarity analysis, and network-based analysis and matched with the cheating behaviours. Finally, they showed that how they can detect cheaters with machine learning algorithms.

This paper provides extensive research on various occurrence cheating methods and solutions for detecting cheaters in MMORPGs.

2.2 Robust Vision-Based Cheat Detection in Competitive Gaming [6]

In the paper "Robust Vision-Based Cheat Detection in Competitive Gaming" we can explore an already existing solution that tries to tackle the cheating problem in Counter Strike - Global Offensive, and another first-person shooter game. The main idea of this method of cheat detection is using DNNs (deep neural networks) to look for rendered frames, that give away visual evidence of a cheating software being used. This can be information in the game that the player should not have (seeing otherwise invisible enemies through walls, or on the map), or the GUI (graphical user interface) of the cheat itself.

The way it is implemented is very straightforward, yet novel. The GPU's frame buffer is captured right before it appears on the computer screen, and is analyzed by a trained DNN. The DNN is trained to look for altered and suspicious pixel patterns. The model's training took place on a large set of frames from the games with and without cheats. It calculates both the probability of a frame containing cheats and the confidence value, which is used both to avoid false positives and to help the developers know when the model needs to be retrained, for example when a cheat software got changed, to avoid detection.

The results were auspicious: The more visually prominent the cheating was, the better the system got at successfully detecting the presence of cheats. Different configurations were mentioned, and the exact results varied based on the configuration in use. The highest overall accuracy measured was 0.89. The developers noted, that this implementation should be used as an extension of already existing cheat detection methods. Overall in my opinion it is a great way to deal with cheaters in online games, and it is worth exploring further when it comes to AI cheat detection.

2.3 Deep learning and multivariate time series for cheat detection in video games [8]

This research introduces a novel cheat detection system for online video games that, instead of traditional in-game data, is based on human-computer interaction (HCI) data, such as keystrokes and mouse movements. Existing systems use game-specific customization to detect cheating, while this approach uses player interaction data as multivariate time series analyzed by convolutional neural networks (CNNs). This makes the system adaptable to various games and capable of detecting cheaters without any game-specific information. The method successfully identifies cheats like aimbots and triggerbots in first-person shooter (FPS) games by recognizing behavioral patterns that differ from typical human interactions.

The study was performed on data collected from players of Counter-Strike: Global Offensive, achieving detection rates of 99.2% for triggerbots and 98.9% for aimbots. Cross-validation was used to ensure the model's robustness and ability to adapt to new player inputs, demonstrating its effectiveness in real-world scenarios. The use of universal input data makes this system, compared to other systems, a flexible and scalable solution for cheat detection. This makes it easy to apply to other games without the need for any specific tuning. This research provides significant advancements in cheat detection methodologies by a game-independent approach that can also adapt to new and evolving forms of cheating.

2.4 Explainable AI for Cheating Detection and Churn Prediction in Online Games [9]

The paper explores the application of AI and XAI (eXplainable AI) in online gaming, focusing on issues such as game cheating detection and player churn prediction. It discusses how AI has historically been applied in games for tasks like matchmaking and behaviour monitoring. XAI specifically addresses the black-box nature of AI models, enhancing trust by providing explanations for AI decisions. The authors introduce datasets from NetEase Games, using a large amount of game logs, player behaviour sequences, client images, and social graphs to improve the transparency and accuracy of AI models.

The authors concluded that the use of XAI could be preferred over the black-box model having received more positive feedback from game operators and game designers alike for its' transparency in reasoning and explanation. These results are far better than the authors expected and they claim that this technology should be further examined and developed to achieve even better results.

3 Background

3.1 Fundamental concepts

3.1.1 What is a multiplayer game?

A multiplayer game is a type of video game that allows multiple players to interact and compete with or against each other in a shared virtual environment. In these games, players usually compete with each other for the best ranking, highest score or reward. Sometimes individually, but sometimes they play together as a team. With the rise of online gaming, cheating has become a major problem in multiplayer games, disrupting the fairness and balance that developers work so hard to achieve. Cheating in these games usually involves players using or exploiting unauthorized means to gain an unfair advantage over others, which can ruin the experience for everyone involved and the game itself.

For example, in the popular game Counter-Strike: Global Offensive (CS), some players use aimbots to automatically aim and shoot [3], removing the need for skill and giving them an unfair edge in competitive matches. Another common form of cheating can be seen in Fortnite, where some players use wallhacks [7] to see enemies through walls, allowing them to prepare ambushes or avoid conflicts that would normally be unavoidable. Game developers actively combat these issues by implementing anti-cheat software and regularly banning accounts that are found cheating. However, as technology advances, so do the methods of cheating, so it's a constant challenge for developers to keep multiplayer games fair and enjoyable. Despite these efforts, cheating remains a persistent problem that affects players' enjoyment.

3.1.2 XAI concepts

Explainable Artificial Intelligence (XAI) is a technology designed to make AI models more transparent and understandable to humans. Traditional AI, especially deep learning, often functions as a black box, meaning users cannot easily understand how it reaches its conclusions. Exploring AI's decision-making process helps people apprehend AI decisions more easily. This is the change wich the XAI aims. Transparency from explanations is key in areas such as healthcare, finance, and law, where AI decisions can have significant consequences. For instance, a doctor using an AI system for diagnosing conditions needs to know why the AI recommends a specific treatment.

XAI works through techniques such as feature visualization, where specific factors influencing a decision are highlighted, or surrogate models, which approximate and explain complex models. By making AI systems more interpretable, XAI helps build trust, allowing users to validate or challenge the AI's conclusions. It also helps identify distortions or errors in the model, reducing unintended damage. As AI becomes more embedded in everyday life, XAI plays a critical role in ensuring ethical, fair, and safe use of AI technologies.

3.2 Anti cheating solutions

3.2.1 Non AI anti cheating solutions

Non-AI anti-cheating methods are techniques used by game developers and administrators to prevent or reduce cheating in multiplayer games without relying on artificial intelligence. One of the most common methods is server-side checks, which involve monitoring player actions for suspicious patterns directly on the game's server. This method can detect things like impossible moves or excessively high scores, which often indicate cheating. Another approach is the use of encrypted game files to prevent players from modifying the game code or assets, which is a common way cheaters create unfair advantages.

Game developers also use measures such as integrity checking, which regularly checks that players' game files are the same as the original, preventing the use of modified or hacked files. Hardware bans are another powerful deterrent that prevents a specific device from accessing the game if cheating is detected. Additionally, some games require players to log in through secured platforms or services, making it difficult to create multiple accounts to cheat. Real-time reporting systems are also common, allowing players to flag suspicious behavior, which is then reviewed by moderators or automated systems. Temporary or permanent bans for cheaters are also widespread, often used as a warning to others. Finally, some games use periodic updates and patches that not only fix bugs, but also potential

exploits that cheaters might use. Together, these methods help maintain fairness in multiplayer games, even without advanced AI-driven solutions.

3.2.2 Best AI anti cheating solutions

AI-driven anti-cheat methods have become extremely effective in detecting and preventing cheating in online multiplayer games. These systems use machine learning algorithms to monitor player behavior and identify anomalies that indicate cheating. One prominent example is Activision's Ricochet anti-cheat system [2] used in Call of Duty games, which uses machine learning to detect irregular gameplay patterns, such as unnatural aiming or movement speed. By analyzing massive amounts of data from legitimate and cheating players, Ricochet can flag suspicious behavior with high accuracy and adapt to new cheating methods quickly.

Another successful AI-based approach is employed in Valorant, a popular first-person shooter developed by Riot Games. Its anti-cheat system, Vanguard [1], incorporates both traditional methods and AI, focusing on both client-side monitoring and server-side detection. AI models analyze player input and game data in real-time, comparing it to normal patterns to detect cheating, such as aimbots or wallhacks. This proactive approach enables Vanguard to detect previously unseen cheats, improving system adaptability to evolving threats.

AI anti-cheat systems also utilize deep learning to detect boosting, where players artificially inflate their rank. For instance, FACEIT, an online competitive gaming platform, uses machine learning to track suspicious ranking progressions and automatically flag accounts for review [4].

These AI methods are more efficient than traditional ones because they can continuously learn from new data, increasing their accuracy over time. However, developers still face the challenge of ensuring privacy and data security while using these powerful tools. By combining real-time analysis and continuous adaptation, AI-based anti-cheat systems significantly improve the fairness and integrity of online gaming experiences.

4 Methodology

We based our anti-cheat system on the use of Deep-Neural-Networks (DNN). In order to understand what a DNN is, first we have to mention ANNs. ANN stands for Artificial Neural Network, and it is a neural network model that is inspired by the structure of the human brain. They consist of three types of layers : Input, Hidden and Output.The input layer takes in raw data, while the output layer produces the result. The hidden layer is an intermediary layer, that helps process the data by applying weights and biases. With that said, a DNN, or Deep Neural Network is a more advanced kind of ANN. The main difference is the depth. A DNN has multiple hidden layers, hence the name "Deep". Deep Neural Networks are capable of completing way more complex tasks than simple ANNs. These tasks can range from image recognition all the way to language processing. The learning process of a DNN is similar to that of an ANN. It involves training the network by adjusting the hidden layer weights, based on the end result.

We used DNNs to analyze player behavior and look for irregular gameplay patterns. To achieve this we used large training datasets of player behavior from cheaters and legitimate players. Our model looks at several behavior patterns that can indicate cheating, such as players looking through walls, inhuman reaction times, abnormal movement patterns. This includes both "spinbotting" and aiming using abnormally straight lines, since humans can't draw perfectly straight lines with their mouse movement. Our system also utilizes user input analysis, which can detect illegal keyboard or mouse macros.

We have also used convolutional neural networks to help detect cheaters. During the AI model's training, we have used data based on players' interactions, and in-game data. These consisted of behavioral analysis, such as highly precise and fast movements and other anomalies. Using a large scale of inputs from both cheating and normal players, this model learns these differences and can differentiate them.

To verify the model's accuracy and efficiency, we used cross-validation. This helped us test the model by splitting the data into multiple sets. This has ensured that there is no overfitting and helped this model perform better compared to what it was capable of before. In our experiment, we found that the 5-fold or 10-fold cross-validation was more effective, and mostly these were used during training.

The model's results were highly accurate, with a very small percentage of false positives. This CNN model has helped the whole cheat detection system advance in this territory as well. Using this model, aim bots and trigger bots are mostly caught giving a new depth to our cheat detection.

We applied XAI technology along with the other AI models to receive feedback from our anti-cheat system. Our intention was to severely reduce the amount of false positives and to eliminate misconduct from our anti-cheat system. The feedback XAI generates provides a reason proving the validity of the detection system, this feedback is also visible to game operators and the developers so they can fine-tune or overrule the anti-cheat system, further reducing misconduct in certain cases of system alerts or flags.

Behavioural tracking and evolution tracking was also implemented in our system. By tracking player statistics and success rate we further improved the accuracy of cheat detection. Sudden changes in a player's statistics over a given period of time indicates some form of cheating, which could show that the player uses game cheats or that another player is using their account. XAI helps in determining the exact cause of the flagging, this way the player receives the appropriate punishment.

Behavioural tracking proves long-term analysis of the players' actions increases the accuracy of the anti-cheat system, but in order to give players the best experience and to ensure the competitive integrity of games we trained our model to provide low-latency real-time cheat detection. To train our system we used small fragments of game data at a time to improve response time and the reliability of low-latency decisions.

...

5 Discussion

The usage of DNNs showed impressing results in anti-cheat detection for games. With the help of DNNs we applied image recognition during gameplay and could determine illegal or cheat-likely movement and accurately decide whether a player is cheating or not. The usage of image recognition showed interesting results on how cheat developers trick currently used anti-cheat systems. The combination of AI models we implemented trains itself with the newly fed user data and improves the detection of unusual player movements. Analysing user input helped with gaining a deeper understanding of the average user input and the average actions of a player. This proved useful in anti-cheat detection, because unlikely or missing inputs for certain game actions showed that a player was cheating with a great success rate. The DNN solutions could identify obvious cheating with a 95% accuracy. This shows that DNN models are powerful tools in combating cheating in video games.

...

Our studies have shown that the use of XAI, along with other models delivers a more reliable and verifiable source for cheat detection. When used with real-time detection, XAI proved slower and less responsive, yielding less accurate reasons for cheating. Given enough training it could improve and provide accurate explanations along with the real-time cheat detection models.

...

6 Conclusion

...

7 Future Work

Even though we tried using the most advanced technologies currently available, there are still a lot of ways to improve upon the anti-cheat detection system we implemented. We tried to train the AI models with as much data as possible, but implementing this detection system in a popular video game and using the available user data from a larger player base could further improve the models' accuracy. The usage of even more or diverse AI models could enhance the effectiveness of this system. ...

References

[1] Jan Bohnerth. How anti-cheat systems try to save online video games. 2021.

[2] Arianna Boldi and Amon Rapp. "is it legit, to you?". an exploration of players' perceptions of cheating in a multiplayer video game: Making sense of uncertainty. *International Journal of Human–Computer Interaction*, 40(15):4021–4041, 2024.

[3] Minyeop Choi, Gihyuk Ko, and Sang Kil Cha. BotScreen: Trust everybody, but cut the aimbots yourself. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 481–498, Anaheim, CA, August 2023. USENIX Association.

[4] FACEIT. What is faceit anti-cheat and how does it work?, 2023. Accessed: 2024-10-27.

[5] Mee Lan Han, Byung Il Kwak, and Huy Kang Kim. Cheating and detection method in massively multiplayer online role-playing game: Systematic literature review. *IEEE Access*, 10:49050–49063, 2022.

[6] Aditya Jonnalagadda, Iuri Frosio, Seth Schneider, Morgan McGuire, and Joohwan Kim. Robust vision-based cheat detection in competitive gaming. *Proceedings of the ACM on Computer Graphics and Interactive Techniques*, 4(1):1–18, 2021.

[7] Seonghyun Park, Adil Ahmad, and Byoungyoung Lee. Blackmirror: Preventing wallhacks in 3d online fps games. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 987–1000, New York, NY, USA, 2020. Association for Computing Machinery.

[8] José Pedro Pinto, André Pimenta, and Paulo Novais. Deep learning and multivariate time series for cheat detection in video games. *Machine Learning*, 110(11):3037–3057, 2021.

[9] Jianrong Tao, Yu Xiong, Shiwei Zhao, Runze Wu, Xudong Shen, Tangjie Lyu, Changjie Fan, Zhipeng Hu, Sha Zhao, and Gang Pan. Explainable ai for cheating detection and churn prediction in online games. *IEEE Transactions on Games*, 15(2):242–251, 2022.