Eötvös Loránd University

Faculty of Informatics

Dept. of Software Technology and Methodology

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

Supervisor:
John Doe
Assistant Lecturer

Author:
Gémesi Szabolcs, Görcsös Gergely, Nagy Ri
Computer Science BSc

Budapest, 2024

Contents

Chapter 1

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.

Chapter 2

Literature review

2.1 Cheating and Detection Method in Massively Multiplayer Online Role-Playing Game: Systematic Literature Review [1]

The main topic of this review is the examination of possible fraud in MMORPG games, the exploration of its causes, introduction of its types and presentation of a possible detection method.

In MMORPG games, a stateful game server is used, the three characteristics of which are presented in the research. First, all clients must be connected to the server, because the server provides real-time data to the client. Second, the in-game and user data are all saved in the server-side memory. Third, all the logic is done by the server side, it saves and reads to its own memory. Due to this, if the game crashes before saving, data loss may occur.

The article describes four methods of fraud, which it intends to solve together. The first of these is the use of game sticks. It divides bots into two classes, hardware and software, and also defines two types: in-game and out-of-game bots. The second fraud method is the use of an illegal private server, which means a server that can provide similar content as the original. The illegal private server causes massive user churn and direct economic damage to game developers and publishing companies. The third fraud method presented is the theft of user accounts. They can obtain significant amounts of an unfair advantage by conducting cash transactions with a game user's online information through account theft. The fourth method is Gold

Farming Groups and Real Money Trading. Gold farming involves cheating to acquire game items by mobilizing inexpensive labor. Real money trading is a rational economic activity owing to the differences in opportunity costs, and it serves a mediating role between the virtual world and real-world economies. However, Real money trading can also be used to mediate illegal transactions owing to the enhancement and diversification of cheating in online games.

The review gives us two types of countermeasures. The first one is based on the server side part. For this, the server is separated into three parts: client-side, network-side, and server-side. The other provides countermeasures against cheating behavior. In the process of doing this, it sets up a behavior pattern about the user, from logging in to logging out.

Finally, it presents the detection possibilities. He classifies these into five groups: statistics analysis, data mining, similarity analysis, and network-based analysis.

The statistical technique is generally based on the measurement of variance, mean, standard deviation, distribution, p-value, and z-value from separately classified log data for the features applicable to all MMORPG. It gives an advantage to the statistical technique, which is to detect cheating game users regardless of the game user's playing period.

Data mining in MMORPGs was used as a decision-making technique to correlate data and extract meaningful information by analyzing game behavior factors, such as game playing patterns.With this, it is possible to protect game bots, since their relatively simple behavior can be easily analyzed. The similarity analysis technique can also be a suitable method for analyzing bots. It checks the presence or absence of cheating by analyzing the similarity between the game user's current behavior and his/her previous behavior.

Network-based analysis can be used to produce a relational map of a network comprising of nodes and edges. Suprisingly game users who mainly perform cheating behavior called gold farming by gold farmers and RMT have weak social connections as compared with normal game users.

Finally they presented a machine learning that are used in their respective research and what results can be derived from them: Decision Tree, Support Vector Machine (SVM), Naïve Bayes, K-Nearest Neighbors (KNN), Bayesian network, AdaBoost, and Multilayer Perceptron.

This study provides extensive research on various occur- rence cheating methods

as well as methods for detecting MMORPGs. From a structural framework point of view, considering the stateful game server and conceptual attributes of MMORPGs, it explains in detail whether MMORPGs are structurally prone to cheating

2.2 Robust Vision-Based Cheat Detection in Competitive Gaming [2]

The online first-person shooter game, Counter-Strike 2 (Formerly known as Counter-Strike: Global Offensive) is infamous for its cheating problem and scandals. There have been several instances of professional players getting caught cheating on stage. 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. One of the major advantages of this method of cheat detection is its regard for privacy. Most anti-cheat software accesses the whole memory, leaving room for potential privacy breaches and data leaks. Some anti-cheats also operate on the kernel level (Vanguard - Valorant). If these are coded poorly and can be exploited they can create severe security vulnerabilities. Compared to these solutions visual cheat detection can be considered less intrusive, and more safe regarding data protection. 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 men-

tioned, 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 [3]

This research focuses on developing a novel cheat detection system for online video games that uses human-computer interaction (HCI) data instead of traditional in-game data. In most anti-cheat systems, detecting cheating activity uses analyzing game-specific data, such as player positioning or in-game behavior, which requires manual customization for each game. The puropose of this research is an alternative, not game-specific method, which detects cheating with the monitoring of player interactions with hardware. The hardware monitoring relies on keystrokes and mouse movements. This approach avoids the limitations of game-specific systems, making it fit to various video games.

The key innovation lies in treating player interactions as multivariate time series data. This is then analyzed using convolutional neural networks (CNNs). CNNs are particularly suited to recognizing patterns in irregular and complex data, just like human behavior. By using this method, the researchers try to identify behavioral patterns that differentiates legitimate players from cheaters. This system targets two types of cheats: aimbots (which automatically target opponents) and triggerbots (which fire weapons as soon as a target is aligned). These cheats highly alter player behavior, particularly mouse movement and reaction times, making them detectable through interaction data alone. This detection method is suited for FPS (first person shooter) games.

In this experiment, the authors relied on data collected from players of the game Counter-Strike: Global Offensive. The dataset included interaction data from regular and cheating players, focusing on keyboard and mouse activity. The system has achieved detection rates of 99.2% for triggerbots and 98.9% for aimbots, making this approach highly effective. Unlike previous cheat detection models, which often rely

on in-game data and are limited to specific environments, this system's reliance on universal input data makes it highly flexible and scalable across different games and even potentially applicable to other domains involving human-computer interaction.

The research also used cross-validation to ensure that the model adapts well to new players inputs. This is important for new player inputs, so that the model doesn't works only on the pre-trained data. This helps the model's accuracy on real scenarios, on unfamiliar players.

This study provides several contributions. It proposes a cheat detection method that does not rely on game data but uses only HCI events, which allows application across various games and helps adapt to new forms of cheating. The approach enhances the existing body of research on cheating detection by using a more advanced and effective method, as it uses multivariate time series data that are processed by CNNs. This method not only improves the accuracy of existing systems, but also has broader applications in other areas where users could be simulated by interaction data.

2.4 Explainable AI for Cheating Detection and Churn Prediction in Online Games [4]

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.