Research on the Application of Artificial Intelligence in Online Game Anti-Cheating

Lehan Li[a]
Institute of Problem Solving, Chongqing University of Posts and Telecommunications, Chongwen Road, Nan'an District, Chongqing, China

Keywords: Anti-Cheating, Game Security, Artificial Intelligence, Online Games.

Abstract: In recent years, the popularity of online games has made anti-cheating systems particularly important. Although the traditional anti-cheating system has formed a relatively perfect system after years of development and iteration, with the update of hardware and software and the popularity of AI, cheating methods are also iterating rapidly. The use of Artificial Intelligence (AI) and Direct Memory Access (DMA) to cheat has become a popular option for cheaters, while traditional anti-cheating systems have little effect. This paper reviews the application of artificial intelligence in anti-cheating in online games, analyses the advantages and disadvantages of existing methods, and looks forward to the future development trend. By using artificial intelligence technology, game developers and researchers can more efficiently analyse the data in the game to determine whether players cheat, and can also assist the anti-cheating process by analysing players' text information. Therefore, combining artificial intelligence with anti-cheating can more effectively detect and prevent cheating in online games, to maintain the fairness of the game and the good experience of players.

1 INTRODUCTION

Online games have become increasingly popular in recent years, and many companies' businesses revolve entirely around their online games and the consistent revenue generated accordingly. If there are a large number of cheaters in a game, it will seriously affect the ecology of the game and the revenue of the company, but also cause great damage to the reputation of the game and even the reputation of the company.

Anti-cheating system is helpful to provide better game experience for players. After years of development and iteration, the traditional anti-cheating system has formed a relatively perfect system to deal with cheating in online games. However, with the update of hardware and software and the popularity of AI, cheating methods are also iterated rapidly, and the use of AI and external equipment DMA cheating has become a general trend of cheating development, and for these new cheating means, the effect of traditional anti-cheating systems is minimal. In this context, game developers and researchers began to experiment with artificial intelligence technology to detect and prevent cheating. Around the world, many researchers have begun to explore the use of artificial intelligence technology to combat cheating in online games. For example, in their study in 2013, Alayed and Frangoudes et al used machine learning technology to analyze the data transmitted between the client and the server, calculate the eigenvalue, and judge whether the user has cheating behavior through the calculated results (Alayed et al., 2013). In a 2022 study, Kanervisto and Kinnunen et al designed a deep learning approach to control a computer mouse to enhance a player's level of play and investigated its effectiveness against cheating (Kanervisto et al., 2022). In their 2022 study, Tao and Xiong et al proposed a workflow called GAXI, this approach leverages the capabilities of multi-view data sources while also benefiting from the clarity and transparency offered by multi-view black box models, and has good results in game cheating detection on real-world data sets (Tao et al., 2022). In his 2017 study, Maguluri proposed a general automatic player classification method based

[a] https://orcid.org/0009-0004-8363-7345

Li, L.
Research on the Application of Artificial Intelligence in Online Game Anti-Cheating.
DOI: 10.5220/0013234500004558

In *Proceedings of the 1st International Conference on Modern Logistics and Supply Chain Management (MLSCM 2024)*, pages 106-111
ISBN: 978-989-758-738-2

on artificial intelligence technology and natural language processing to classify players as cheaters/victims/neutralists based on the text of their statements on social platforms to aid the anti-cheating process (Maguluri, 2017).

These studies show that artificial intelligence technology has broad application prospects in the field of anti-cheating. However, with the continuous evolution of cheating methods, anti-cheating systems are also facing new challenges. In the future, anti-cheating systems will need to continuously incorporate the latest artificial intelligence technology to deal with increasingly sophisticated cheating, maintain the fairness of the game and the good experience of the players.

2 OVERVIEW OF CHEATING TECHNIQUES

In online games, cheating usually refers to the behaviour of players to gain an advantage over their opponents or achieve certain goals by modifying the game or using other improper means (Yan, & Randell, 2005). These cheating behaviours not only destroy the fairness of the game, but also may seriously affect the game experience of other players and the reputation of the game company.

In their research on the classification of cheating in online games in 2005, Jeff and Brian mentioned the definition of player cheating: players who violate the rules set by game operators and gain more advantages than other players through illegal means are regarded as cheating (Jeff & Brian, 2005).

2.1 Traditional Cheating Methods

In the game, every object (including characters, buildings, props, etc.) is a 3D model generated by a computer, and these models have a memory store, which includes the location of the model, state and other information.

Traditional cheats are usually done by reading the game's memory, such as:

- Perspective cheating: By modifying or reading the game's memory data, the player can "see" information that is not normally visible. For example, by reading the position information of other player models, it is possible to "see" each other from behind a wall, which is called "perspective".
- self-aiming cheating: by reading the data in the memory, obtain the position information of other players, and then through calculation, automatically adjust the player's aiming Angle and shooting time, so that players can easily hit each other.

In the classification study on cheating in online games in 2005, Jeff and Brian sorted out 15 types of plug-in categories according to the potential vulnerabilities, consequences and cheating principles (Jeff & Brian, 2005), which almost completely showed the ways and harms of traditional cheating methods.

2.2 Novel Cheating Methods

With the continuous development of technology, the continuous update of hardware and software, and the popularity of AI, cheating methods are also in rapid iteration. Among them, the use of AI cheating and DMA cheating has begun to take shape, and the inability of traditional anti-cheating methods has caused the proliferation of AI cheating and DMA cheating in today's online games, which has a serious impact on the game ecology, company reputation and revenue.

2.2.1 Using AI to Cheat

AI cheating uses artificial intelligence techniques (such as machine learning, deep learning, etc.) to achieve game cheating. Compared with traditional cheating methods, AI cheating is more intelligent and hidden. The principle is as follows:

- Image recognition: By capturing the game screen, AI can identify enemies, items and other information in the game according to the trained model. This method does not directly read the game memory, more difficult to detect by the anti-cheat system.
- Decision and operation: AI makes decisions (such as moving, aiming, shooting, etc.) according to the identified information, and then implements cheating functions by simulating player operations (such as simulating keys, mouse operations, etc.). This mode of operation is closer to real player operation, reducing the risk of detection.

2.2.2 Using DMA to Cheat

DMA cheating is a way to realize game cheating through hardware devices. DMA cheating equipment can obtain or modify game data by directly accessing game memory, so as to achieve cheating effect. The principle is as follows:

- Hardware devices: DMA cheating requires specialized hardware devices, such as PCIe devices and USB devices. These devices can access computer

memory directly without the intervention of the operating system.

- Memory access: DMA devices read or modify game data (such as player position, aiming Angle, etc.) by directly accessing game memory to achieve cheating effect. Because of the hardware-level access, it is difficult to be detected by the anti-cheat system.
- Drivers: In order to realize the interaction between the DMA device and the game, a special driver is also needed. These drivers generally need to bypass the operating system's security mechanisms in order to be able to access protected memory areas.

3 ANTI-CHEATING METHODS

3.1 Traditional Anti-Cheating Methods

In order to maintain the good ecology of online games, the anti-cheating system is one of the unattainable links. The anti-cheating system in online games refers to a set of technologies and measures aimed at detecting, preventing and combating game cheating, the main purpose of which is to maintain the fairness, stability and game experience of players.

Traditional anti-cheating methods mainly rely on the monitoring, analysis and processing of game data and player behaviour to identify and combat cheating, including the following principles: abnormal data detection, behaviour pattern recognition, client-side integrity verification, plug-in program detection, server-side verification, blacklist system.

In a 2020 study, Lehtonen analysed the common anti-cheating methods used in online games today, and rated the anti-cheating methods based on tamper-proof, ease of implementation, lack of overhead, non-intrusion, and suitability for various games (Lehtonen, 2020).

3.2 Artificial Intelligence Anti-Cheating Methods

As cheating methods continue to evolve, traditional anti-cheating methods may not be effective in some cases against new types of cheating such as AI or DMA. Therefore, modern anti-cheating systems often combine artificial intelligence technology to improve the accuracy and real-time detection of cheating.

3.2.1 Use Artificial Intelligence Technology to Efficiently Analyse Data and Identify Cheating

Alayed et al. proposed a method by setting characteristic values to data, using artificial intelligence technology to analyse the data transmitted between the client and the server, calculate the characteristic values, and judge whether the user has cheating behaviour through the calculated results.

From the experimental data of the author in Table1, it can be seen that the analysis of data between client and server based on artificial intelligence method has a high detection rate for cheating methods such as Lock, Auto-Switch, Auto-Miss, Slow-Aim and Auto-Fire.

The anti-cheating method proposed by Alayed et al. effectively uses artificial intelligence technology to better and more efficiently analyse the data between the client and the server to determine whether players' cheat. However, the core of this method is still to analyse the normal transmission of data in the game, which is not good for the detection of cheating methods that do not use traditional data transmission such as AI dual machine /DMA cheating.

3.2.2 Use Artificial Intelligence Technology to Analyse Coordinate Information Aimed at Players to Determine Cheating

Willma proposes an RNN-based deep learning algorithm (Willman, 2020) that analyses the coordinates that a player is aiming at to determine if an Aimbot is being used to cheat.

Table 1: Accuracy results for Part 4 (Alayed et al., 2013).

Cheat Type	Best Selected Results				
	TPR for L	TPR for AF	TPR for Normal	Frame Size	Classifier
L	96.6%	2.4%	100%	60	SVM-RBF
AS	100%	0%	100%	60	Both
AM	89.7%	0%	100%	60	SVM-RBF
SA	89.7%	0%	100%	60	Both
AF	55.2%	100%	96.9%	60	SVM-L

The anti-cheating method proposed by Willman is no longer confined to the analysis of the transmission data between the client and the server, and opens the idea of artificial intelligence in anti-cheating methods. Unfortunately, it is mentioned in the paper that the target accuracy of the algorithm should be over 90% in order to truly identify whether a player is cheating with Aimbot (Willman, 2020), but the author of the paper only achieved an accuracy of slightly over 50% due to time and data set limitations. Whether this method can be used in existing online games still needs to be studied.

Pinto et al. introduced sophisticated anti-cheating methods utilizing artificial intelligence that are very flexible yet substantially dependent on in-game data. Consequently, each game must incorporate an adaptive anti-cheating system(Pinto et al., 2021).

Pinto et al., therefore, propose a new cheat detection method that does not rely on in-game data (pinto et al., 2021). The approach initially analyzes the multimodal interactions between the player and the platform as multivariate time series. Subsequently, it employs a CNN network to classify these time series and ascertain if the game player has engaged in cheating behaviour.

The contribution of the article can be summarized as follows:

- New techniques for detecting cheating in video games only based on input data, such as keystrokes and mouse movements, which are derived from player behaviour.
- CNN structure to detect cheating in a supervisory manner.
- Create data collection and processing methods for human-computer interaction multivariable time series restatements.

Kanervisto et al. designed an AI method (GAN-Aimbot - GAN-generated adversarial network) to control a computer mouse to enhance the player's level of play, and studied its effectiveness against cheating. At the same time, an automatic cheat detection mechanism (VACNet) built using DNN networks is also introduced, which can automatically detect cheating players by detecting whether players cheat only through mouse movement coordinate data (Kanervisto et al., 2022).

The experimental results in this paper show that the test results of Aimbot designed based on GAN are much better than those of ordinary Aimbot, and the automatic cheating detection system built based on DNN network has better performance on both training set and test set.

It can be seen that whether it is cheating or anti-cheating, artificial intelligence technology can bring more obvious improvements.

3.2.3 Construct AI Workflow for Anti-cheating

Tao et al proposed the concept of XAI (eXplainable AI) and also proposed the workflow of GXAI (Tao et al., 2022). As shown in Figure 1, this process combines the power of a multi-view data source with the clear transparency of a multi-view black box model.

This study introduces four distinct classifiers and interpreters that analyse character portraits, behaviour sequences, client images, and social graphs. It can be seen from the author's experimental data in the table 2 that XAI has a good effect on anti-cheating detection in four dimensions.

Tao and his team's approach, as discussed in their paper, has been applied and utilized in three real-world applications in NetEase games. These include generating evidence and reasons, debugging and testing models, and compressing and comparing models. User studies have given it highly favourable feedback. This confirms the practicality of using AI in combating cheating in online games.

3.2.4 Use Artificial Intelligence Technology to Analyse the Player's Speech Text to Distinguish Cheating Players

Maguluri studied various natural language processing and artificial intelligence methods as well as text classification tools in his 2017 article, and then proposed a general automatic player classification method to distinguish cheating players (Maguluri, 2017).

The main contribution of this paper is the design of a general automatic player classification method based on natural language processing and artificial intelligence methods to classify players as cheaters/victims/neutrals based on the text of their statements on social platforms to aid the anti-cheating

Table 2: User studies for evidence and reason generation (Tao et al., 2022).

Job	PortraitExplainer	BehaviorExplainer	ImageExplainer	GraphExplainer
Game cheating detection				
Game operator teams	95.9%	90.1%	96.4%	81.1%
Game designer teams	83.1%	76%	88.6%	68.3%

process.

In a 2019 paper, Hughes et al. applied natural language processing (NLP) tools to automate post types Automatic classification of post types (Hughes et al., 2019). It also creates a systematic data processing framework for analysing large unstructured forum data sets.

The main purpose of the method proposed in this paper is to classify users through their statements on social media and analyse whether the users are likely to commit crimes in real life. This method can also be used for anti-cheating in online games. By setting the labels of game cheaters, analysing the players' speeches in game forums, and classifying cheating players, it can also assist the anti-cheating process.

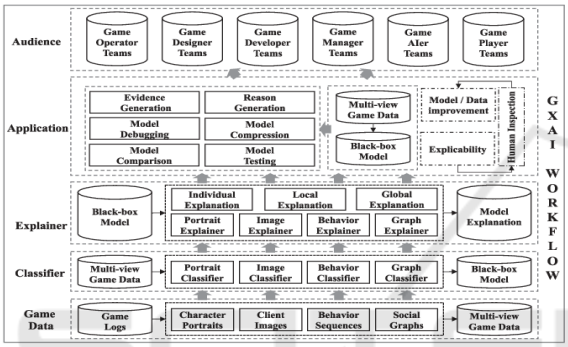

Figure 1: Proposed GXAI Workflow (Tao et al., 2022).

4 CHALLENGES AND PROSPECTS

In recent years, artificial intelligence technology has made remarkable achievements in the field of anti-cheating in online games. However, with the increasing renovation and sophistication of cheating methods, AI technology still faces many challenges and opportunities in future anti-cheating applications.

- More application of artificial intelligence technology: Artificial intelligence technology has made breakthroughs in image recognition, natural language processing and other fields, and is expected to play a greater role in anti-cheating online games in the future.
- Introduction of reinforcement learning technology: Reinforcement learning technology may become an important means of anti-cheating in online games in the future. By analysing game data in real time, reinforcement learning models can automatically detect potential cheating behaviour and adjust according to the cheater's strategy to achieve dynamic anti-cheating. In a paper published in 2022, Lukas et al used reinforcement learning techniques to build an anti-cheating system (Lukas et al., 2022) that could distinguish between robots and normal players in a game, but did not apply the method to anti-cheating in online games. Lukas's approach opens up the idea of using reinforcement learning techniques in online game anti-cheating, which can be used in the future to build an online game anti-cheating system and further strengthen the learning ability of anti-cheating systems to combat cheating methods that are difficult to combat with conventional means such as AI or DMA.
- Integration of cross-field technologies: The application of artificial intelligence technology in anti-cheating online games will continue to expand, involving more related fields. For example, the integration of big data analysis, image recognition, natural language processing and other technologies will help improve the comprehensiveness and accuracy of cheating detection.
- Personalized anti-cheating strategies: With the development of artificial intelligence technology, future anti-cheating systems will be more intelligent and personalized. Through in-depth analysis of player behaviour and game data, the anti-cheating system can provide customized anti-cheating strategies for different types of players, improving game fairness and user experience.

5 CONCLUSION

This paper first introduces the difference between traditional cheating methods and new cheating methods, and then compares and analyses the difference between traditional anti-cheating methods and the new era anti-cheating methods using artificial intelligence. This paper explains the important role of artificial intelligence technology in dealing with the modern and novel cheating methods in online games, and introduces in detail the different ways of applying artificial intelligence technology in the field of anti-cheating and the efforts and results made by predecessors in this direction.

At the same time, the paper also puts forward the future prospect of the research content, which can seek breakthroughs in the application of more artificial intelligence technology, the introduction of reinforcement learning technology, the integration of cross-domain technology and personalized anti-cheating strategies, improve the performance of artificial intelligence technology in the field of anti-cheating in online games, and effectively combat the

currently difficult to solve AI/DMA cheating methods. Optimize the game ecosystem and protect the interests of players and game companies.

REFERENCES

Alayed, H., Frangoudes, F., & Neuman, C., 2013, August. Behavioral-based cheating detection in online first person shooters using machine learning techniques. In *2013 IEEE conference on computational inteligence in games (CIG)* (pp. 1-8). IEEE.

Kanervisto, A., Kinnunen, T., & Hautamäki, V., 2022. Gan-aimbots: Using machine learning for cheating in first person shooters. *IEEE Transactions on Games*, *15*(4), 566-579.

Yan, J., & Randell, B., 2005, October. A systematic classification of cheating in online games. In *Proceedings of 4th ACM SIGCOMM workshop on Network and system support for games* (pp. 1-9).

Willman, M., 2020. Machine Learning to Identify Cheaters in Online Games. *URL http://urn. kb. se/resolve*.

Lehtonen, S., 2020. Comparative study of anti-cheat methods in video games. *University of Helsinki, Faculty of Science*.

Pinto, J. P., Pimenta, A., & Novais, P., 2021. Deep learning and multivariate time series for cheat detection in video games. *Machine Learning*, *110*(11), 3037-3057.

Tao, J., Xiong, Y., Zhao, S., Wu, R., Shen, X., Lyu, T., ... & Pan, G., 2022. Explainable ai for cheating detection and churn prediction in online games. IEEE Transactions on Games, 15(2), 242-251

Maguluri, N. S. N., 2017. Multi-class classification of textual data: Detection and mitigation of cheating in massively multiplayer online role playing games.

Hughes, J., Collier, B., & Hutchings, A., 2019, November. From playing games to committing crimes: A multi-technique approach to predicting key actors on an online gaming forum. In *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-12). IEEE.

Lukas, M., Tomicic, I., & Bernik, A., 2022. Anticheat system based on reinforcement learning agents in unity. *Information*, *13*(4), 173.